LightPointe™ FlightSwitch
Optical Wireless Switch

Installation and Configuration Manual

LIGHTPOINTE™

505-016663-00000 Rev B

2006-01

Copyrights and Disclaimer

Information in this document is provided in connection with LightPointe products. These materials are provided by LightPointe as a service to its customers and may be used for information purposes only. LightPointe assumes no responsibility for errors or omissions in these materials. LightPointe may make changes to specifications and product descriptions at any time, without notice. LightPointe makes no commitment to update the information and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to its specifications and product descriptions.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in LightPointe Terms and Conditions of Sale for such products, LightPointe assumes no liability whatsoever.

These materials are provided "as is" without warranty of any kind, either expressed or implied, relating to sale and/or use of LightPointe products including liability or warranties relating to fitness for a particular purpose, consequential or incidental damages, merchantability, or infringement of any patent copyright or other intellectual property right. LightPointe further does not warrant the accuracy or completeness of the information, text, graphics or other items contained within these materials. LightPointe shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials.

LightPointe products are not intended for use in medical, lifesaving or life sustaining applications. LightPointe customers using or selling LightPointe products for use in such applications do so at their own risk and agree to fully indemnify LightPointe for any damages resulting from such improper use or sale.

The following are trademarks of LightPointe Product names or services listed in this publication are for identification purposes only, and may be trademarks of third parties. Third-party brands and names are the property of their respective owners.

FlightLite™, FlightPath™, FlightStream™, FlightStrata™, FlightPower™, FlightManager™ and FSO™ are trademarks of LightPointe.

LightPointe believes the printed matter contained herein to be accurate from date of publication and reserves the right to make changes as necessary without notice

Reader Response: LightPointe strives to produce quality documentation and welcomes your feedback. Please send comments and suggestions to LightPointe. For technical questions, contact your local LightPointe sales office or field applications engineer.

Table of Contents

List of Figures

List of Tables

Intended Readers

The LFSW-3226L Manual contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Typography	Description
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the File menu and choose Cancel. Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the copy command.
Menu Name > Menu Option	Indicates the menu structure.
Device > Port > Port Properties	Means the Port Properties menu option under the Port menu option that is located under the Device menu.

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions.

Observe and follow service markings. Do not service any product except as explained in your system documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock. Only a trained service technician should service components inside these compartments.

If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:

- The power cable, extension cable, or plug is damaged.
- An object has fallen into the product.
- The product has been exposed to water.
- The product has been dropped or damaged.
- The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.

- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage selection Switch (if provided) on the power supply is set to match the power available at your location:

  – 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan

  – 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan

  – 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  – Install the power supply before connecting the power cable to the power supply.

  – Unplug the power cable before removing the power supply.

  – If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.

- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

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

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

Caution: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack.

After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.
- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.

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

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

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

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

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.

When transporting a sensitive component, first place it in an antistatic container or packaging.

Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads and an antistatic grounding strap.

Service

There are no serviceable parts within the unit. Only factory trained personnel can provide service on any internal components of the Switch.

Warranty

LightPointe warrants this product against faulty materials or workmanship under the terms of our current Standard Warranty And Support Agreement provided that the product was purchased directly from us or from one of our authorized resellers. Please contact LightPointe Customer Service for additional information or to obtain a copy of the Warranty Agreement.

Contacting LightPointe

Corporate Office

10140 Barnes Canyon Road, San Diego, CA 92121
Phone: 858.643.5200, Fax: 858.643.5201

Technical Support

Phone: (U.S.) 858.643.5299

Website: www. LightPointe.com

Email: techsupport@LightPointe.com

Using This Manual

This manual describes how to install and configure the LightPointe LFSW-3226L Fast Ethernet Switch.

Section	Contents
1. System Overview	System functional and physical overview
2. Switch Configuration	Detailed step-by-step installation, configuration, and alignment procedures
3. Overview of Basic Switch Settings	Detailed overview of basic Switch settings
4. Troubleshooting and Diagnostics	Resolving operational problems
5. Specifications	Physical and electrical specifications
6. Index	Keyword index
Appendix A	Glossary
Appendix B	Advanced Switch Settings

Additional Resources

Refer to the following documents for additional information about the LightPointe system.

Document Number	Title
505-015902-00000	Field Engineering and Planning Guide
505-016300-00000 Rev A	FlightLite 100/100E Installation and Maintenance
505-004148-00000	FlightLite 155E Installation and Maintenance
505-015408-00000	FlightLite G Installation and Maintenance
505-004148-00000	FlightStrata 52E/52EW
505-004148-00000	FlightStrata 155E/155EW
505-015494-00000	FlightStrata 622
505-015494-00000	FlightStrata G
505-016662-00001 Rev A	FlightStrata 100 XA Installation and Maintenance

1. Introduction

This chapter covers the following main topics:

- Switch Overview
- Switch Description

1.1. Switch Overview

The LFSW-3226L switch is used with all LightPointe link heads to handle failover in Dual-Path (link head and RF) installations, to minimize flapping, and to provide basic network management functionality.

This switch is modified for use with LightPointe systems. It is not intended to be used as a standard network switch. Changing switch configuration and parameters can impact LightPointe products and performance.

Note: Certain switch functions may not be available in all LightPointe systems configurations. Please refer to the corresponding section of the manual for additional information.

1.2. Switch Description

1.2.1. Unshielded Twisted Pair Ports (UTP)

The LightPointe LFSW-3226L Switch is equipped with 24 unshielded twisted-pair (UTP) cable ports providing dedicated 10 or 100 Mbps bandwidth. For link heads with a fiber interface, an optical-to-ethernet media converter must be used. When selectinga media converter, ensure fiber type, bandwidth, optical power and wavelength match the link head.

- UTP ports are used for connecting link heads and other networking devices.
- UTP ports and Auto MDI-X/MDI-II convertible ports can be used for uplinking to another Switch.
- The dual speed ports use standard twisted-pair cabling and are ideal for segmenting networks into small, connected subnetworks for superior performance.
- Each 10/100 port can support up to 200 Mbps of throughput in full-duplex mode.

1.2.2. Mini-GBIC Combo Ports

In addition, the Switch has 2 Mini-GBIC (Gigabit Interface Connector) combo ports. These two-gigabit combo ports are ideal for connecting to a LightPpointe Gigabit link head, server or network backbone.

1.2.3. Switch Features and Benefits

- Multiple Port Options – 24 10/100Mbps Fast Ethernet ports and 2 combo 10/100/1000Mbps SFP/mini-GBIC ports allow connection to all LightPointe linkheads – copper and fiber (with media converter), Fast Ethernet and Gigabit.
- Superior Failover Management – ideal for installations requiring a radio backup link for redundancy.
- Rapid Spanning Tree Protocol – provides fast and efficient switching from primary to secondary links in the event of link failure or interruption.
- Flapping Reduction – RSTP and enhanced switch software minimize port flapping and enables switch to maintain link connection even during multiple failovers.
- Voice and Data Traffic Support – built-in QoS (Quality of Service) capabilities makes switch suitable for both data and VoIP (voice over IP) environments.RJ-45 Copper Interface; SFP/Mini-GBIC.
- Network Management - supports all standards-based network management protocols (SNMP, RMON, BOOTP, Telnet, Web) to ease integration into a variety of third party network management packages.
- High Capacity – Switching fabric is cable of handling up to 8.8 Gbps of data traffic to meet growing traffic requirements.
- Rack-Mountable Design – simplifies installation into existing network cabinets and equipment configurations.
- Advanced Functionality – additional switch features such as QoS, link aggregation, port-based authentication, VLANs are also available for enhanced network functionality.
- IEEE 802.3 10BASE-T and 802.3u 100BASE-TX compliant
- IEEE 802.1p Priority Queues
- IEEE 802.3x flow control in full duplex mode
- IEEE 802.1x Port-based Access Control
- IEEE 802.1Q VLAN
- IEEE 802.1D Spanning Tree support
- High performance Switching performs forwarding and filtering at full wire speed, maximum 14, 881 packets/sec on each 10Mbps Ethernet port, and maximum 148,810 packet/sec on 100Mbps Fast Ethernet port.
- Full- and half-duplex for both 10Mbps and 100Mbps connections. Full duplex allows the Switch port to simultaneously transmit and receive data. It only works with connections to full-duplex-capable end stations and Switches. Connections to a hub must take place at half-duplex
- Support broadcast storm filtering
- Non-blocking store and forward Switching scheme capability to support rate adaptation and protocol conversion

- Supports by-port Egress/Ingress rate control
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed
- Support port-based enable and disable
- Address table: Supports up to 4K MAC addresses per device
- Supports a packet buffer of up to 3 Mbits
- Supports Port-based VLAN Groups
- Port Trunking with flexible load distribution and fail-over function
- Supports Link Aggregation Control Protocol
- Supports port segmentation
- IGMP Snooping support
- Port Mirroring support
- MIB support for:

  - RFC1213 MIB II
  - RFC1493 Bridge
  - RFC1757 RMON
  - RFC1643 Ether-like MIB
  - RFC2233 Interface MIB
  - Private MIB
  - RFC2674 for 802.1p
  - IEEE 802.1x MIB

- RS-232 DCE console port for Switch management
- Provides parallel LED display for port status such as link/act, speed, etc.

Ports

- Twenty-four (24) high-performance (MDI-X/MDI-II) ports.
- All UTP ports can auto-negotiate between 10Mbps and 100Mbps, half-duplex and full duplex, and feature flow control.
- Two 1000BASE-T Mini-GBIC combo ports for connecting to another Switch, server, or network backbone.
- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

1.2.4. Front-Panel Components

The front panel of the Switch consists of LED indicators for power and for each 10/100 Mbps twisted-pair ports, and two 1000BASE-T Mini-GBIC ports.

Figure 1-1: Front Panel View of the LFSW-3226L

Comprehensive LED indicators display the status of the Switch and the network.

LED Indicators

The LED indicators of the Switch include Power, Console, Link/Act, Speed and FDX. This Switch also includes a LED Mode button, which has the default setting set to Link/Act. The user may scroll through to show the LED status for Link/Act, Speed and FDX of each port. The following Figure shows the LED indicators for the Switch along with an explanation of each indicator.

Figure 1-2: LED Indicators

Table 1-1: LED Indicators

	Back Panel LEDs	Description
A	Power	Green after the Switch is powered on Dark when the Switch is powered off

	Back Panel LEDs	Description
B	Console	Blinks during the Power-On Self Test (POST). When the POST is finished, the LED goes dark Solid amber when the POST test has failed Solid green when the Switch is being logged into via out-of-band/local console management through the RS-232 console port in the back of the Switch using a straight-through serial cable
C	Port LEDs	One row of LEDs for each port is located above the ports on the front panel First LED is for the top port and the second LED is for the bottom port Light accordingly with the Link/Act, Speed and FDX options chosen with the LED Mode button
D	Link/Act	When the LED mode set to Link/Act: ❑ Steady green to indicate a valid link ❑ Blinking LED indicates activity on the port.
E	Speed	When LED mode set to Speed: ❑ Steady green indicates the port is transferring data at 100Mbps ❑ When the light is unlit, the port is transferring at a rate of 10Mbps For the two Mini-GBIC speed LEDs: ❑ A steady green light indicates the port is transferring data at 1000Mbps ❑ An unlit LED indicates a transfer rate of 100Mbps or 10Mbps.
F	FDX	When LED mode set to FDX: ❑ Steady green indicates that the port is transferring data at full duplex ❑ When the light is unlit, the port is transferring at half-duplex.

Rear Panel Description

The rear panel of the Switch contains an AC power connector. The AC power connector is a standard three-pronged connector. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 ~ 240 VAC at 50 ~ 60 Hz.

Side Panel Description

The right-hand side panel of the Switch contains two system fans. The left-hand side panel contains heat vents.

The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation.

Caution: Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

Gigabit Combo Ports

In addition to the 24 10/100 Mbps ports, the XA Switch features two Gigabit Ethernet Combo ports. These two ports are 1000BASE-T copper ports and Mini-GBIC ports also known as SFP (Small Form Pluggable) GBICs. There are two types of mini-GBIC modules:

- LX mini-GBIC – Conforms to the 1000Base-LX standard
- SX mini-GBIC – Conforms to the 1000Base-SX standard

IMPORTANT NOTE

Media Converters and SFP Mini-GBICs are NOT included with the FlightSwitch product. To obtain a list of recommended Media Converters or SFP Mini-GBICs, please contact your local LightPointe sales representative or partner.

These modules act as media converters translating fiber interfaces and other types of gigabit signals into a common format. GBIC connectors plug into switches, routers to change interface capabilities without changing boards or replacing equipment. GBIC Please note that although these two front panel modules can be used simultaneously, the ports must be different. The GBIC port will always have the highest priority.

The two Mini-GBIC combo ports are ideal for uplinking to a network backbone or server. The copper ports operate at a speed of 1000, 100 or 10Mbps in full or half duplex mode. The fiber optic ports can operate at 1000Mbps in full and half duplex mode.

Connections to the Gigabit Ethernet ports are made using fiber optic cable or Category 5 copper cable, depending on the type of port. A valid connection is indicated when the Link LED is lit.

Figure 1-3: Mini-GBIC Ports

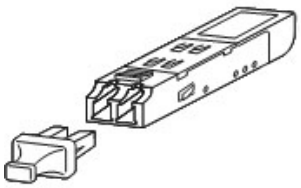


Figure 1-4: Mini-GBIC Module

2. Switch Configuration

This chapter covers the following main topics:

- Switch Configuration Data
- Bench Test Set Up - Equipment and Interconnection
- Switch Configuration using the RS-232 Console Port
- Optional QoS Set up (Priority Queuing of Frame Packet Data)
- Optional SNMP Set Up (Version 1 or 2c)
- Switch Configuration using a Web Browser

2.1. Introduction

All software function of the LFSW-3226L Switch can be managed and configured using standard Command Line Interface commands or through a web-based interface. Each LFSW-3226L Switch is assigned a unique MAC address that cannot be changed. This ensures that MAC addresses remain consistent in the event of failovers. The MAC address can be viewed using the "show switch" CLI command or by opening the Switch Web management program and select the Switch Information (Basic Settings) window on the Configuration menu.

The LFSW-3226L uses Rapid Spanning Tree Protocol to seamlessly and rapidly switch between links especially in dual-path (optical wireless + RF environments). In most instances switching is done in sub-seconds.

IMPORTANT NOTE

The LFSW-3226L switch has been customized and preconfigured to ensure optimal performance in LightPointe-specific Optical Wireless installations. Any changes to default settings, port assignments, use of advanced switch features or use of non-LightPointe linkheads or radios may impact system operation and will not be supported by LightPointe.

2.1.1. Embedded WEB-Based (HTML) Interface

The Switch can be managed from remote stations anywhere on the network through a standard browser. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

- The web-based configuration screen (Figure 2-1) can be accessed by entering the switch IP address (default 192.168.1.102 for local/root switch, 192.168.1.202 for remote/ non-root switch)
- All settings encountered in web-based management are the same as those found in the console program.

NOTE: For FlightStrata 100 XA installations only, the link head, switch and radio can be accessed and modified through FlightManager XA

software. All other non-XA installations require that each component be configured through their respective configuration tools

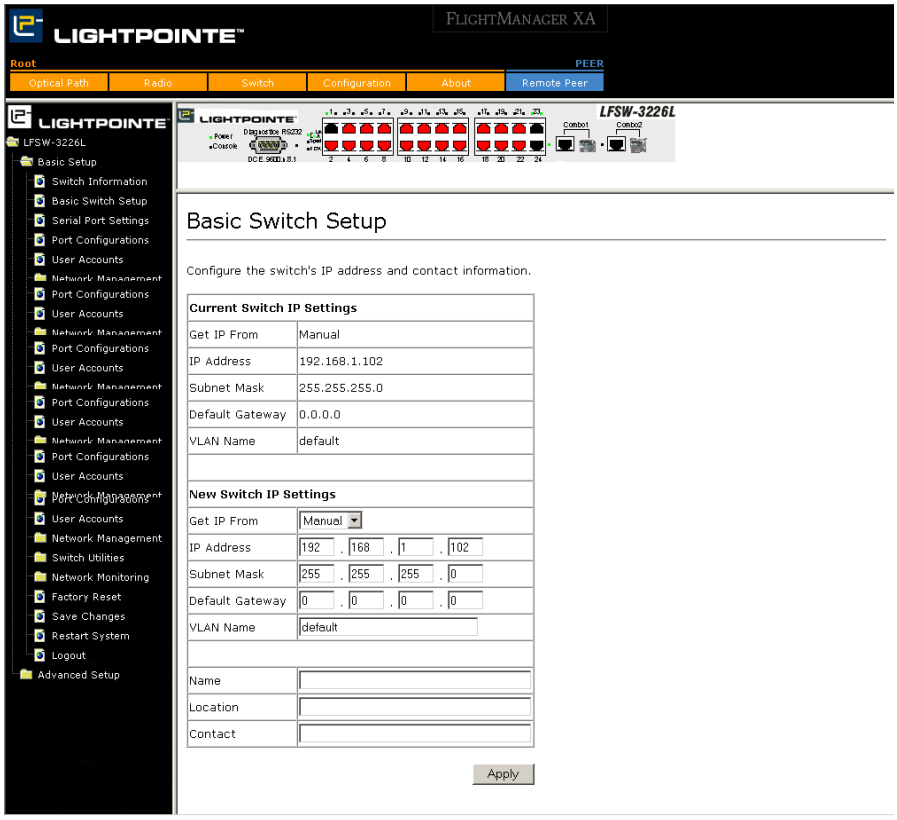


Figure 2-1: Web-Based LFSW-3226L Switch Configuration Screen

2.1.2. Console Program

The LFSW-3226L internal switching software can be configured using standard console management interface commands. The console management interface allows you to connect to the switch's management agent via a serial port and a terminal or a computer running a terminal emulation program.

2.1.3. Telenet Interface

Once the LFSW-3226L Switch has been assigned an IP address, the console can be used over the network using a TCP/IP Telnet program (in VT-100 compatible terminal mode) to access and control the switch. All of the screens are identical, whether accessed from the console port or from a Telnet interface.

2.2. Network Management

One of the key features of the LFSW-3226L Switch is the ability to track network performance including link up/down status and other measurement criteria through the various switch ports.

The LFSW-3226L Switch supports all standards-based network management protocols (SNMP, RMON, BOOTP, Telnet, Web) to ease integration into a number of third party network management packages.

- For FlightLite 100/100E installations, basic network management such as link/up down, packet throughput and transmit/receive information can be tracked through the switch port. The FlightLite 100/100E link heads cannot be managed directly through the switch.
- For all fiber-based link heads including the FlightLite 155, FlightStrata 155, FlightLite G and FlightStrata G, basic network management such as link/up down, packet throughput and transmit/receive information can be tracked through the switch port. Additional network management for these link heads is only available through the OMI port using either a direct craft interface or SNMP proxy agent (LDX) and FlightManager PC software.
- For FlightStrata 100 XA configurations, critical link head, radio and switch information is accessible through the FlightManager XA software. Linkhead information includes power level and bit error rates, for example, while radio information includes signal strength (RSSI) and transmit/receive data. SNMP traps and alarms can be set through the switch to track these and other key network parameters.

2.3. Configuration Data

Each LFSW-3226L Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application. You can change the default Switch IP address to meet the specification of your networking address scheme.

The following table identifies the required components and network addresses (factory defaults) required to configure a link head.

Table 2-1: Components and Required Network Information

Components	Number Required	IP Address	Description
Laptop Management Console	1 Minimum	(Customer Assigned = XXX) Local: 192.168.1.XXX Peer: 192.168.1.XXX	Pentium 4 or equivalent
LightPointe LFSW-3226L Switch	2	(Factory Configured) Local: 192.168.1.102/24 Peer: 192.168.1.202/24	Layer 2 Switch
LightPointe Radio and Flat Panel Antenna	2	(Factory Configured) Local: 192.168.1.101 Peer: 192.168.1.201	Secondary communications link
LightPointe Link Head (Data Port)	2	Transparent Bridge	Primary communications link
LightPointe Link Head Management Port (If applicable)	2	(Factory Configured) Local: 192.168.1.100 Peer: 192.168.1.200	Management Interface

Customer Assigned IP Address Information

Please record customer assigned IP address information in this section before beginning equipment configuration and installation. Information can also be written on the diagram in Figure 2-2 for easy reference.

Table 2-2: Customer Assigned IP Addresses

Customer Configurable Component	Customer Assigned IP Address
Local Laptop Management Console:	
Peer Laptop Management Console (Optional):	
Local LightPointe Ethernet XA Switch:	
Peer LightPointe Ethernet XA Switch:	
Local LightPointe Radio:	
Peer LightPointe Radio:	
LightPointe Local Link Head Management Port: (If applicable)	
LightPointe Peer Link Head Management Port: (If applicable)	
(Optional) SNMP Server:	

2.3.1. FlightLite 100/100E Bench Test Set Up - Equipment and Interconnection

When to Use LFSW-3226L:

- The Switch is an optional component of the FlightLite 100/100E systems.
- Ideal for use in RF-backup implementations.
- If experiencing lengthy failover times using industry standard switch.
- If ports close (primary link does not recover) due to multiple failovers using industry standard switch.
- If basic network management for FL100/100E is required.

Benefits of LFSW-3226L Switch in this Environment:

- Sub-second failover from primary (optical wireless) to secondary (RF backup) link.
- Configuration, monitoring and network management through a single software interface (FlightManager XA).
- Pre-configured and customized firmware optimizes switch performance and manages multiple failovers without port closure.

Key Requirements/Considerations:

- The LFSW-3226L is rate-limited for optimal use in combination data and voice environments. If data-only traffic is being transmitted, turning the switch QoS features off will result in higher throughput.
- All ports should be in Auto Negotiation mode to ensure highest throughput.

The following figure illustrates how to set up the FlightLite 100/100E systems for bench testing and component pre-configuration. The Switch is factory configured for this system. When setting up the system, use the ports identified in the diagram below.

FLIGHTLITE 100/100E CONFIGURATION

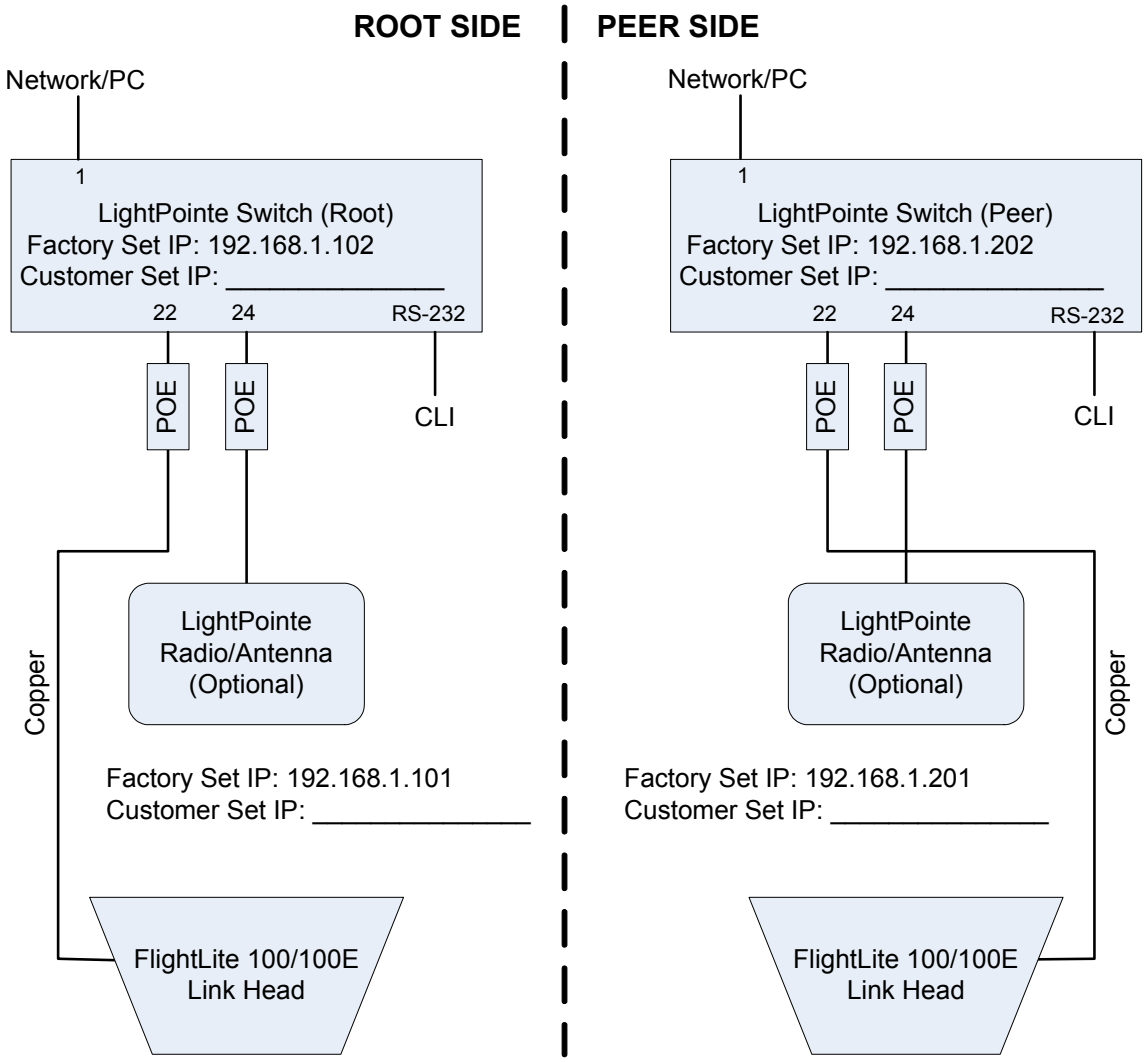


Figure 2-2: FlightLite 100/100E Bench Test Interconnect Diagram

IMPORTANT NOTE

The LFSW-3226L switch has been customized and preconfigured to ensure optimal performance in LightPointe-specific Optical Wireless installations. Any changes to default settings, port assignments, use of advanced switch features or use of non-LightPointe linkheads or radios may impact system operation and will not be supported by LightPointe.

2.3.2. FlightLite 155 and FlightStrata 155 Bench Test Set Up

Benefits of LFSW-3226L Switch in this Environment:

- The Switch is an optional component of the FlightLite 155 and FlightStrata 155 systems.
- Sub-second failover from primary (optical wireless) to secondary (RF backup) link.
- Pre-configured and customized firmware optimizes switch performance and manages multiple failovers without port closure.
- Network management (link up/down, data packet throughput, transmit/receive data) through switch is required.

Key Requirements:

- Optical-to-Ethernet Media Converter - must have link pass-through capabilities and must match the fiber type, bandwidth, optical power and wavelength of the linkhead (sample vendors: Canary, Omnitron, Transition).
- Network management for these link heads is available through the OMI port using either a direct craft interface or an SNMP proxy agent (LDX) and FlightManager PC software.
- The LFSW-3226L is rate-limited for optimal use in combination data and voice environments. If data-only traffic is being transmitted, turning the switch QoS features off will result in higher throughput. Furthermore, all ports should be in Auto Negotiation mode to ensure highest throughput.

The following figure illustrates how to set up the FlightLite and FlightStrata 155 systems for bench testing and component pre-configuration. Each Switch is factory configured for this system. When setting up the system, use the ports identified in the diagram below.

IMPORTANT NOTE

Media Converters and SFP Mini-GBICs are NOT included with the FlightSwitch product. To obtain a list of recommended Media Converters or SFP Mini-GBICs, please contact your local LightPointe sales representative or partner.

FLIGHTLITE 155/FLIGHTSTRATA 155 CONFIGURATION

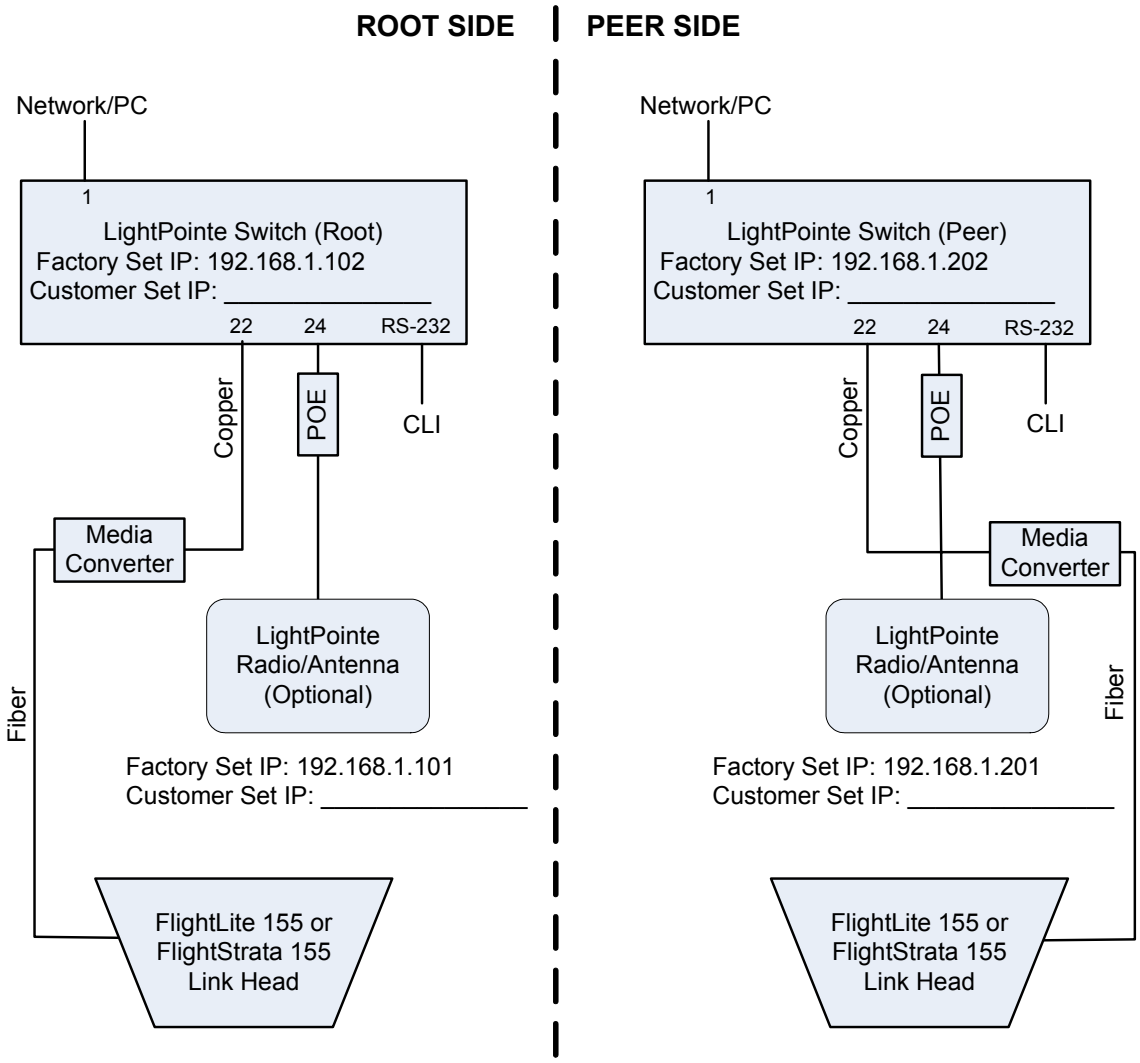


Figure 2-3: FlightLite and FlightStrata 155 Bench Test Interconnect Diagram

IMPORTANT NOTE

The LFSW-3226L switch has been customized and preconfigured to ensure optimal performance in LightPointe-specific Optical Wireless installations. Any changes to default settings, port assignments, use of advanced switch features or use of non-LightPointe linkheads or radios may impact system operation and will not be supported by LightPointe.

Note: Copper to Fiber Media converters must match the fiber type, optical power and bandwidth of the link head.

2.3.3. FlightLite-G and FlightStrata-G Bench Test Set Up - Equipment and Interconnection

When to Use LFSW-3226L:

- The Switch is an optional component of the FlightLite-G and FlightStrata-G systems.
- Ideal for use in RF-backup implementations.
- If experiencing lengthy failover times using industry standard switch.
- If ports close (primary link does not recover) due to multiple failovers using industry standard switch.

Benefits of LFSW-3226L Switch in this Environment:

- Sub-second failover from primary (optical wireless) to secondary (RF backup) link.
- Network management (link up/down, data packet throughput, transmit/receive data) through switch.

Key Requirements:

- SFP/Mini-GBIC for interface between fiber and switch port (must match fiber type).
- An Optical-to-Ethernet Media Converter can be used instead of a GBIC (must have link pass-through capabilities and must match the fiber type, bandwidth, optical power and wavelength of the linkhead).
- Network management for these linkheads is available through the OMI port using either a direct craft interface or an SNMP proxy agent (LDX) and FlightManager PC software.
- The LFSW-3226L is rate-limited for optimal use in combination data and voice environments. If data-only traffic is being transmitted, turning the switch QoS features off will result in higher throughput. Furthermore, all ports should be in Auto Negotiation mode to ensure highest throughput.

The following figure illustrates how to set up the FlightLite-G and FlightStrata-G systems for bench testing and component pre-configuration. Each Switch is factory configured for this system. When setting up the system, use the ports identified in the diagram below.

IMPORTANT NOTE

Media Converters and SFP Mini-GBICs are NOT included with the FlightSwitch product. To obtain a list of recommended Media Converters or SFP Mini-GBICs, please contact your local LightPointe sales representative or partner.

FLIGHTLITE G/FLIGHTSTRATA G CONFIGURATION

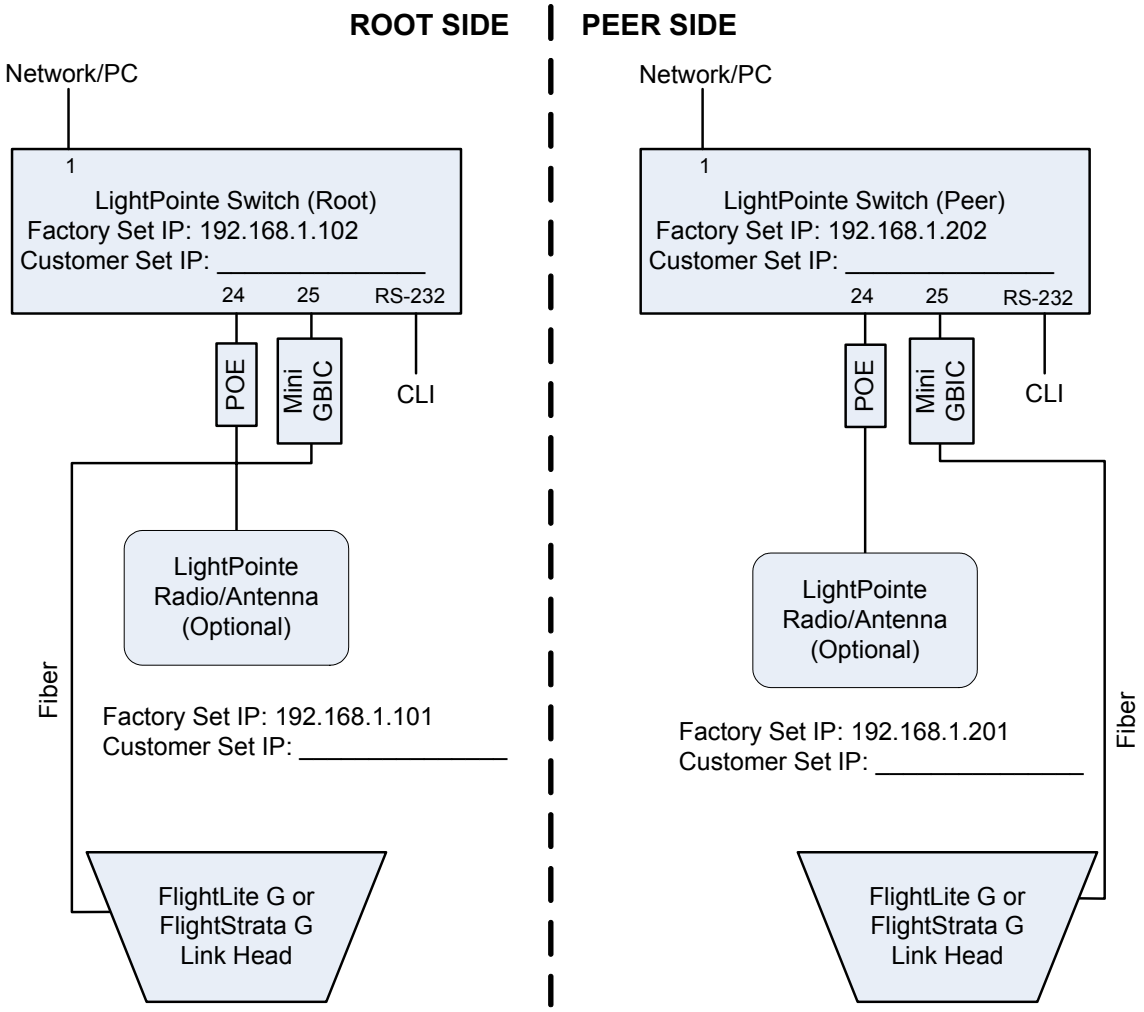


Figure 2-4: FlightLite-G and FlightStrata-G Bench Test Interconnect Diagram

IMPORTANT NOTE

The LFSW-3226L switch has been customized and preconfigured to ensure optimal performance in LightPointe-specific Optical Wireless installations. Any changes to default settings, port assignments, use of advanced switch features or use of non-LightPointe linkheads or radios may impact system operation and will not be supported by LightPointe.

Note: Small Form Pluggable GBICs need to match the fiber type of the link head.

2.3.4. FlightStrata 100 XA Bench Test Set Up - Equipment and Interconnection

When to Use LFSW-3226L:

- The Switch is a standard component of FlightStrata 100 XA.
- Included in all FlightStrata 100 XA system orders.

Benefits of LFSW-3226L Switch in this Environment:

- Sub-second failover from primary (optical wireless) to secondary (RF backup) link.
- Configuration, monitoring and network management through a single software interface (FlightManager XA).
- Pre-configured and customized firmware optimizes switch performance and manages multiple failovers without port closure.

Key Requirements:

- The LFSW-3226L is rate-limited for optimal use in combination data and voice environments. If data-only traffic is being transmitted, turning the switch QoS features off will result in higher throughput. Furthermore, all ports should be in Auto Negotiation mode to ensure highest throughput.

The following figure illustrates how to set up the FlightStrata 100 XA system for bench testing and component pre-configuration. Each Switch is factory configured for this system. When setting up the system, use the ports identified in the diagram below.

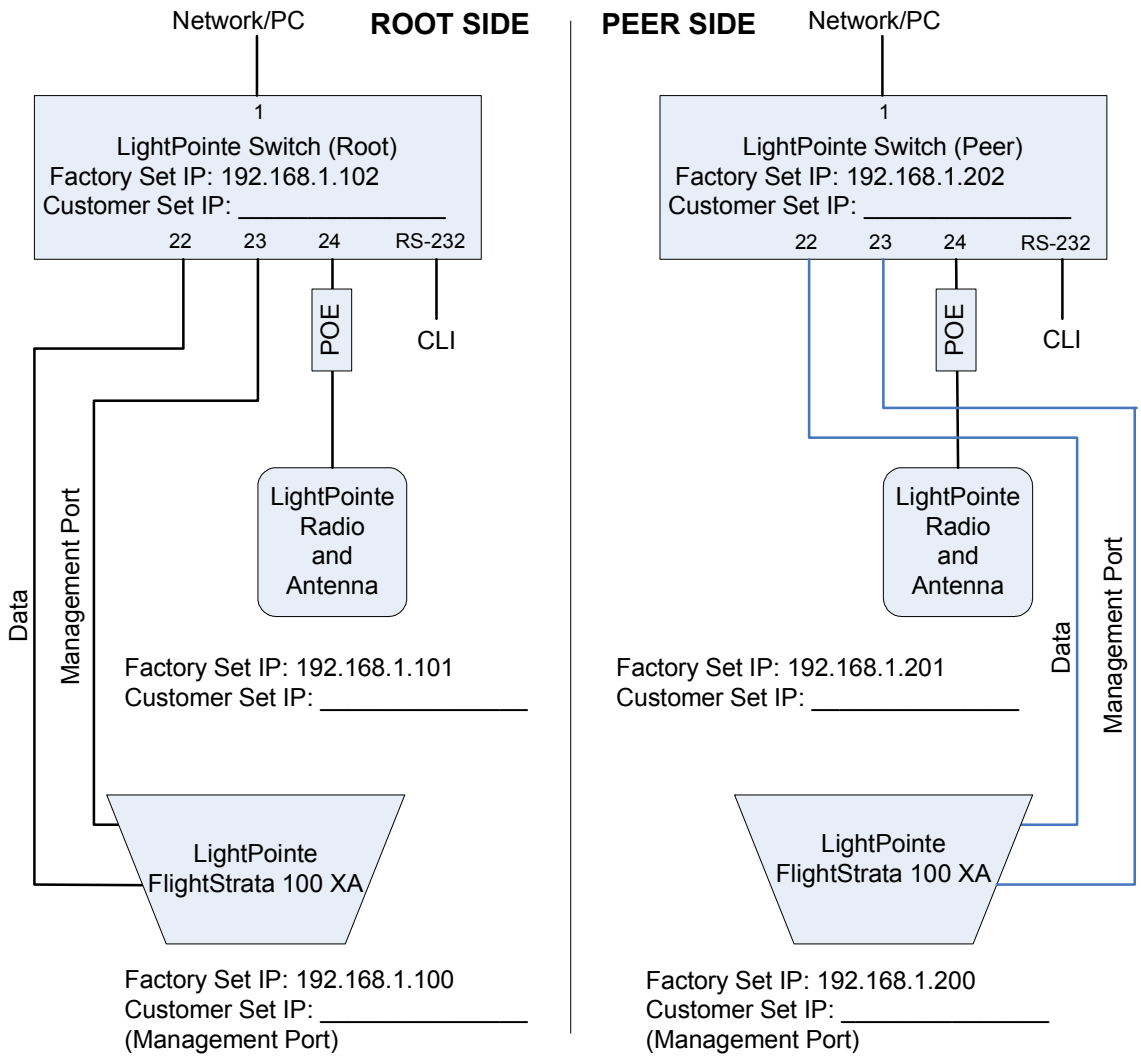


Figure 2-5: FlightStrata 100 XA Bench Test Interconnect Diagram

For FlightStrata 100 XA installations only, the linkhead, switch and radio can be accessed and modified through FlightManager XA software. All other non-XA installations require that each component be configured through their respective configuration tools

IMPORTANT NOTE

The LFSW-3226L switch has been customized and preconfigured to ensure optimal performance in LightPointe-specific Optical Wireless installations. Any changes to default settings, port assignments, use of advanced switch features or use of non-LightPointe linkheads or radios may impact system operation and will not be supported by LightPointe.

2.3.5. Switch Configuration using the RS-232 Console Port

The LightPointe LFSW-3226L Switch may be configured out-of-band through the console port on the front panel. You can connect a computer or terminal to the serial console port to access the Switch.

To use the console port, you need the following equipment:

- A terminal or a computer with both a serial port and the ability to emulate a terminal.
- A null modem or crossover RS-232 cable with a female DB-9 connector for the console port on the Switch.

IMPORTANT NOTE

When you use HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 allows you to use arrow keys in HyperTerminal's VT100 emulation.

The console port command-line-driven interface (CLI) provides complete access to all Switch management features. Configuring the Switch includes the following tasks:

- Set Network IP Address
- Set Per Port data rate limitation
- Enable and disable selected ports
- RSTP Setup
- VLAN QoS setup
- SNMP (Simple Network Management Protocol) setup

RSTP Set up

To set up the Switch to utilize Rapid Spanning Tree Protocol, perform the following steps on both the far and local Switches. All CLI comments are preceded by two forward slashes (i.e. // comment).

Step 1 Ensure the bench test system is interconnected correctly.

- Port #1 – Connected to a Network/PC
- Port #24 – RF Unit (STP Enabled)
- **FlightLite 100/100E/155 and FlightStrata 155/100 XA**
  Port #22 – Linkhead Data (STP enabled)
  or
  FlightLite/FlightStrata G
  Port #25 for "G" Linkheads (STP enabled)

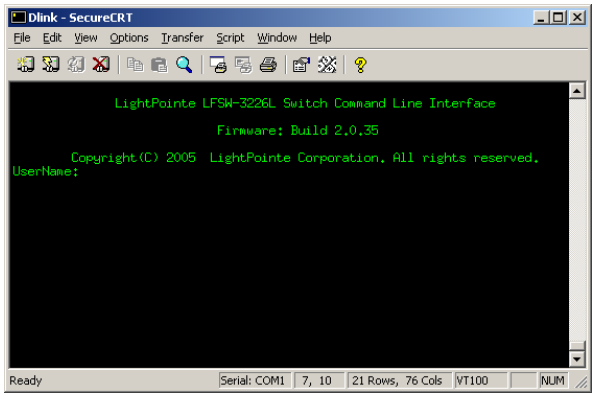
Step 2 Connect a 9-pin RS-232 serial port between the PC serial port and the CLI serial port on the front panel of each LFSW-3226L Switch.

Step 3 Ensure the PC serial port is configured as follows:

- ❑ 9600 baud
- ❑ no parity
- ❑ 8 data bits
- ❑ 1 stop bit

Step 4 Start up a HyperTerminal on the PC. With the serial port and computer properly connected, the following screen should appear.

❑



Note: Press Ctrl+R to refresh the screen. This command can be used at any time to force the console program in the Switch to refresh the console screen.

Step 5 Press the Enter key twice. The CLI cursor **LFSW-3226L:4#** is displayed. This is the command line from which all of the following commands are input.

Step 6 The following commands can be used to display the status of the Switch:

- ❑ Display information about the Switch
  LFSW-3226L:4#show Switch
- ❑ Display the IP address
  LFSW-3226L:4# show ipif
- ❑ Display the port status
  LFSW-3226L:4# show ports
- ❑ Display STP settings
  LFSW-3226L:4# show stp
- ❑ Display STP port settings
  LFSW-3226L:4# Show stp ports

Step 7 Configure the IP Addresses of the Near and Peer Switches. You must use the customer IP addresses. The addresses shown below are the factory default settings.

- ❑ Local:
  LFSW-3226L:4#config ipif System ipaddress 192.168.1.102
- ❑ Peer:
  LFSW-3226L:4#config ipif System ipaddress 192.168.1.202

Step 8 Enable Fast Ethernet ports and disable ports not used.

- **FlightLite 100/100E/155 and FlightStrata 155/100 XA**
  LFSW-3226L:4#config ports 22 speed 100_full
  or
  FlightLite/FlightStrata G
  LFSW-3226L:4#config ports 25 speed 100_full
- **FlightLite 100/100E/155/100 XA**
  LFSW-3226L:4#config ports 2-21, 23 state disable
  or
  FlightLite/FlightStrata G
  LFSW-3226L:4#config ports 2-23 state disable

Step 9 Configure the Switch Spanning Tree Protocol settings for both Switches.

- **LFSW-3226L:4#enable stp**
- Globally enable STP on Switch for rapid spanning tree protocol.
  LFSW-3226L:4#config stp version rstp
- Set the maximum amount of time (in seconds) that the Switch will wait to receive a BPDU packet before reconfiguring STP.
  LFSW-3226L:4#config stp maxage 6
- Set the maximum amount of time (in seconds) that the root device will wait before changing states.
  LFSW-3226L:4#config stp forwarddelay 4
- The time interval between transmission of configuration messages by the root device.
  LFSW-3226L:4#config stp hellotime 1

Step 10

- Set the maximum number of Hello packets transmitted per interval. The count can be set from 1 to 10.
  LFSW-3226L:4#config stp txholdcount 10
- Allow the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch.
  LFSW-3226L:4#config stp fbpdu disable
- Local side - A numerical value between 0 and 61,440 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher the priority.
  LFSW-3226L:4#config stp priority 4096
- Peer side -
  LFSW-3226L:4#config stp priority 8192
- **FlightLite 100/100E/155 and FlightStrata 155**
  LFSW-3226L:4#config stp ports 22 priority 16
  or
  FlightLite/FlightStrata G
  LFSW-3226L:4#config stp ports 25 priority 16
- **FlightLite 100/100E/155 and FlightStrata 155**
  LFSW-3226L:4#config stp ports 1-21, 23 state disable
  or
  FlightLite/FlightStrata G
  LFSW-3226L:4#config stp ports 1-23 state disable
- **FlightLite 100/100E/155 and FlightStrata 155**
  LFSW-3226L:4#config stp ports 22, 24 state enable
  or
  FlightLite/FlightStrata G
  LFSW-3226L:4#config stp ports 24-25 state enable
- Set the transmit bandwidth of port 24 to 15 Mbps.
  LFSW-3226L:4#config bandwidth_control 24 tx_rate 192

Step 11

- ❑ Save all settings.
  LFSW-3226L:4#save

Optional QoS Set up (Priority Queuing of Frame Packet Data)

Ports 23 -26 are by default set as VLAN ports. The QoS (Quality of Service) CLI commands are used to set up the Switch to utilize 802.1p priority queuing. Perform the following steps to implement priority queuing on both the far and local Switches.

Step 1 The Switch default state is QoS On. The following settings are examples only. The actual settings are all customer network specific.

- ❑ Create vlan on the Switch named "voip" with ID of "2".
  LFSW-3226L:4#create vlan voip tag 2
- ❑ Create vlan on the Switch named "data" with ID of "3".
  LFSW-3226L:4#create vlan data tag 3

Step 2

- ❑ **FlightLite 100/100E/155 and FlightStrata 155**
  Add ports to the port list of a previously configured vlan "default".
  LFSW-3226L:4#config vlan default add tag 1, 22, 24

  Add ports to the port list of a previously configured vlan "voip".
  LFSW-3226L:4#config vlan voip add tag 1, 22, 24

  Add ports to the port list of a previously configured vlan "data".
  LFSW-3226L:4#config vlan data add tag 1, 22, 24
  or
  FlightLite/FlightStrata G
  Add ports to the port list of a previously configured vlan "default".
  LFSW-3226L:4#config vlan default add tag 1, 24-25

  Add ports to the port list of a previously configured vlan "voip".
  LFSW-3226L:4#config vlan voip add tag 1, 24-25

  Add ports to the port list of a previously configured vlan "data".
  LFSW-3226L:4#config vlan data add tag 1, 24-25

Step 3

- ❑ Save all settings.
  LFSW-3226L:4#save

Optional SNMP Set Up (Version 1 or 2c)

You can manage the LFSW-3226L Switch with an SNMP-compatible console program. The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch.

SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

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

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

- public - Allows authorized management stations to retrieve MIB objects.
- private - Allows authorized management stations to retrieve and modify MIB objects.

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

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

Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMP v.3 in that SNMP

messages may be encrypted. To read more about how to configure SNMP v.3 settings for the Switch read the section entitled Management.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

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

SNMP Set Up example

Perform the following steps on both the Local and Peer Switches.

Step 1 The following settings are examples only. The SNMP server in the following example has an IP address of 192.168.1.106. The actual SNMP server IP address is customer network specific.

- ❑ Enable SNMP traps.
  LFSW-3226L:4#enable snmp traps
- ❑ Optional - Create a recipient of SNMP traps generated by the Switch's SNMP, set the SNMP version to v2c, and specify packet authorization and encryption.
  LFSW-3226L:4#create snmp host 192.168.1.106 v2c private
- ❑ Optional – Same as above command except SNMP version v1 is used.
  LFSW-3226L:4# create snmp host 192.168.1.106 v1 private

Step 2

- ❑ Save all settings.
  LFSW-3226L:4#save

2.3.6. Switch Configuration using a Web Browser

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a web browser. All settings encountered in web-based configuration are the same as those found in the CLI console program (see section 2.3.1).

IMPORTANT NOTE

The LFSW-3226L switch has been customized and preconfigured to ensure optimal performance in LightPointe-specific Optical Wireless installations. Any changes to default settings, port assignments, use of advanced switch features or use of non-LightPointe linkheads or radios may impact system operation and will not be supported by LightPointe.

Step 1 Ensure the bench test system is interconnected correctly.

- ❑ Port #1 – Connected to a Network/PC
- ❑ Port #24 – RF Unit (STP Enabled)
- ❑ **FlightLite 100/100E/155 and FlightStrata 155/100 XA**
  Port #22 – Linkhead Data (STP enabled)
  or
  FlightLite/FlightStrata G
  Port #25 for "G" Linkheads (STP enabled)

Step 2 Connect an ethernet cable between port 1 and the ethernet port on a PC.

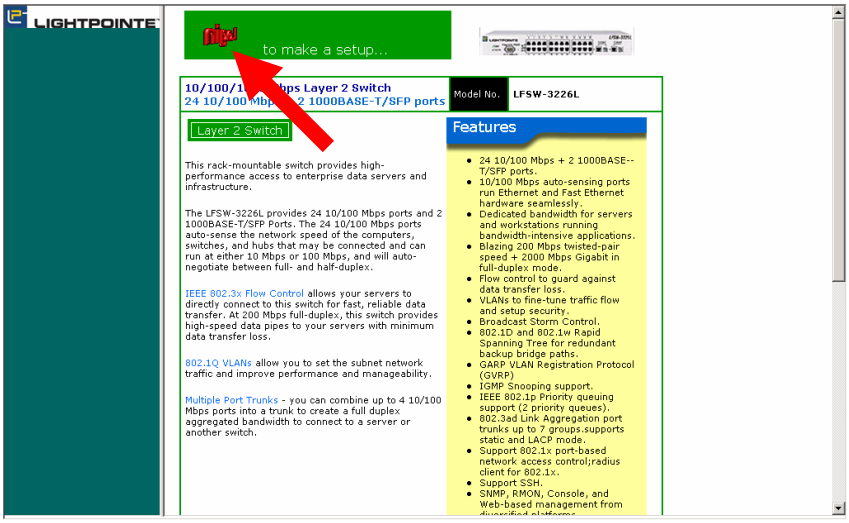
Step 3 Start up a Browser program on the PC.

- ❑ The link heads can be configured using a web browser such as Netscape® Navigator (version 6.2 and higher) or Microsoft® Internet Explorer (version 5.0 and higher)

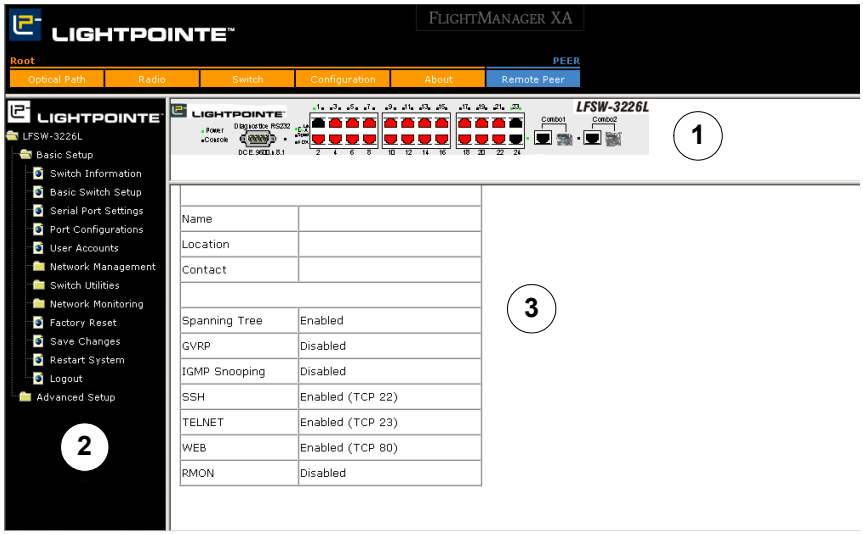
Step 4

- ❑ To open the Switch Web window enter the IP address of the desired Switch (refer to 2.2) in the Browser Location bar. The Switch Web window is displayed.

Step 5 To open the Logon window, click on the spinning logo. The Switch Information window is displayed.

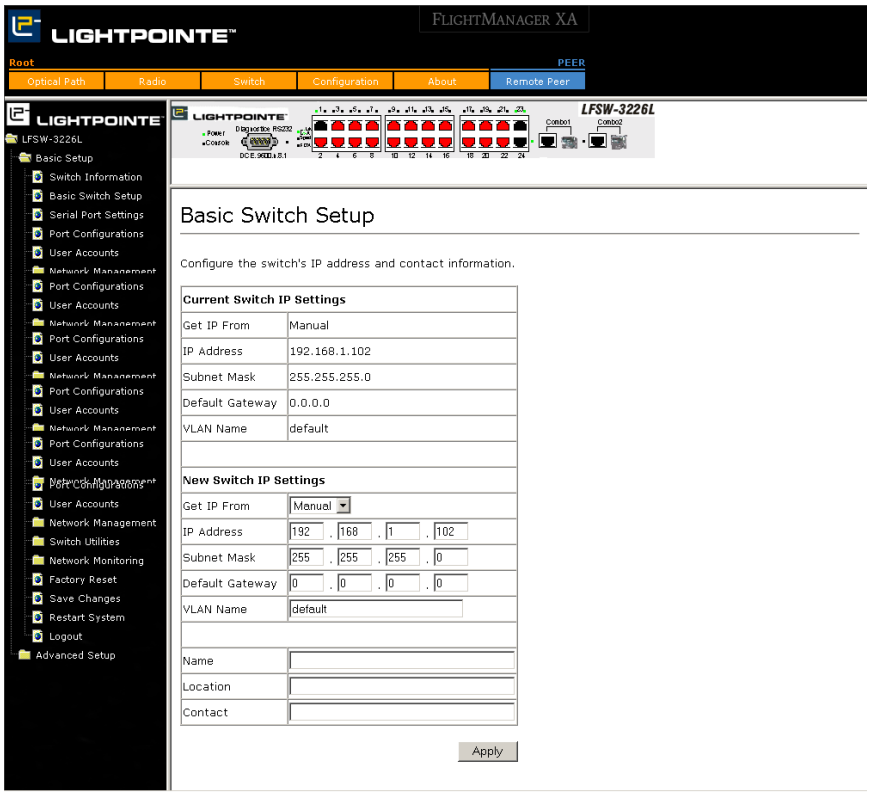


Step 6 The Switch Information window displays the Switch's MAC Address (assigned by the factory and unchangeable), IP configuration, important settings and status information.



- ❑ Pane 1 presents a graphical image of the front panel of the Switch.
- ❑ Pane 2 is used to select the window to be displayed.
- ❑ Pane 3 Displays Switch information based on your selection in Area 2.

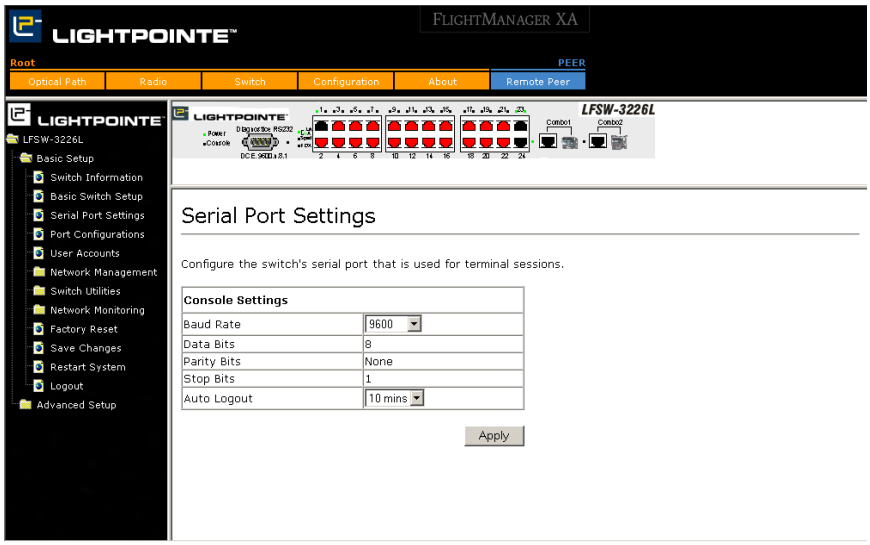
Step 7 Click the **Basic Setup** option in the menu window pane on the left side. The Basic Switch Setup information is displayed.



- ❑ In the **Get IP From** drop-down menu, select **Manual**.
- ❑ Enter the appropriate IP address and subnet mask (see Table 2-1 or Figure 2-2).

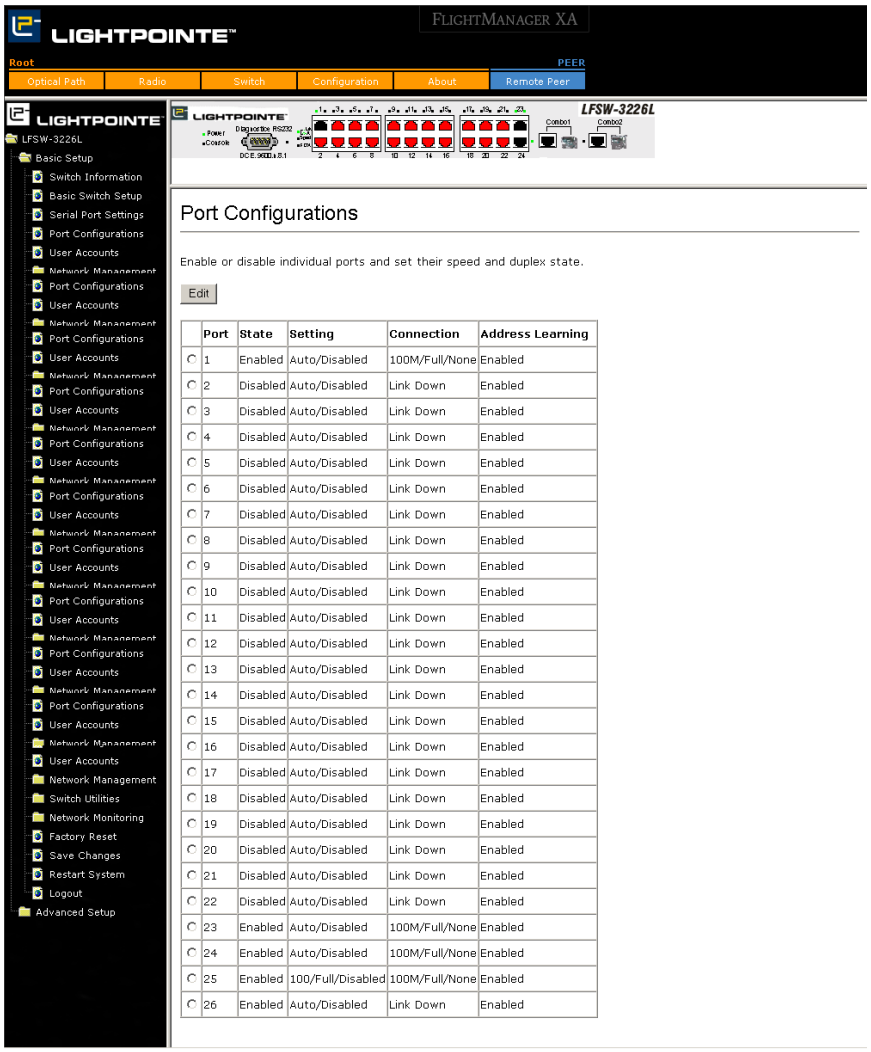
Note: You must use the procedures in Section 2.3.1 if you decide to change the IP Addresses to a new Subnet.

Step 8 Click the **Serial Port Settings** option. The Serial Port Settings window is displayed.



- ❑ Use factory default settings shown above

Step 9 Click the **Port Configuration** option. The Port Configuration window is displayed.

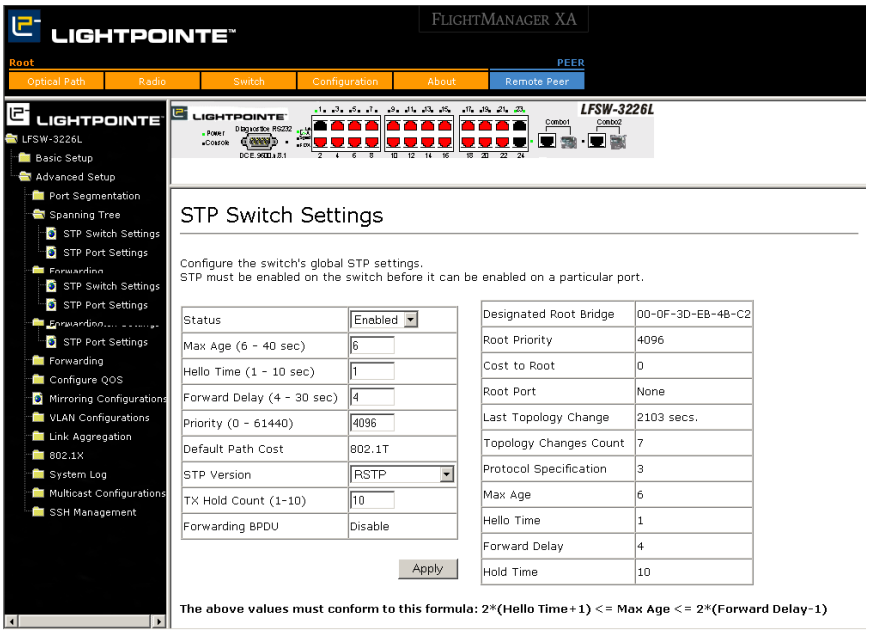


	Port	State	Setting	Connection	Address Learning
○	1	Enabled	Auto/Disabled	100M/Full/None	Enabled
○	2	Disabled	Auto/Disabled	Link Down	Enabled
○	3	Disabled	Auto/Disabled	Link Down	Enabled
○	4	Disabled	Auto/Disabled	Link Down	Enabled
○	5	Disabled	Auto/Disabled	Link Down	Enabled
○	6	Disabled	Auto/Disabled	Link Down	Enabled
○	7	Disabled	Auto/Disabled	Link Down	Enabled
○	8	Disabled	Auto/Disabled	Link Down	Enabled
○	9	Disabled	Auto/Disabled	Link Down	Enabled
○	10	Disabled	Auto/Disabled	Link Down	Enabled
○	11	Disabled	Auto/Disabled	Link Down	Enabled
○	12	Disabled	Auto/Disabled	Link Down	Enabled
○	13	Disabled	Auto/Disabled	Link Down	Enabled
○	14	Disabled	Auto/Disabled	Link Down	Enabled
○	15	Disabled	Auto/Disabled	Link Down	Enabled
○	16	Disabled	Auto/Disabled	Link Down	Enabled
○	17	Disabled	Auto/Disabled	Link Down	Enabled
○	18	Disabled	Auto/Disabled	Link Down	Enabled
○	19	Disabled	Auto/Disabled	Link Down	Enabled
○	20	Disabled	Auto/Disabled	Link Down	Enabled
○	21	Disabled	Auto/Disabled	Link Down	Enabled
○	22	Disabled	Auto/Disabled	Link Down	Enabled
○	23	Enabled	Auto/Disabled	100M/Full/None	Enabled
○	24	Enabled	Auto/Disabled	100M/Full/None	Enabled
○	25	Enabled	100/Full/Disabled	100M/Full/None	Enabled
○	26	Enabled	Auto/Disabled	Link Down	Enabled

Use the factory default settings.

- **FlightLite 100/100E/155 and FlightStrata 155**
  LFSW-3226L:4#config ports 22 speed 100_full
  or
  FlightLite/FlightStrata G
  LFSW-3226L:4#config ports 25 speed 100_full
- **FlightLite 100/100E/155**
  LFSW-3226L:4#config ports 2-21, 23 state disable
  or
  FlightLite/FlightStrata G
  LFSW-3226L:4#config ports 2-23 state disable

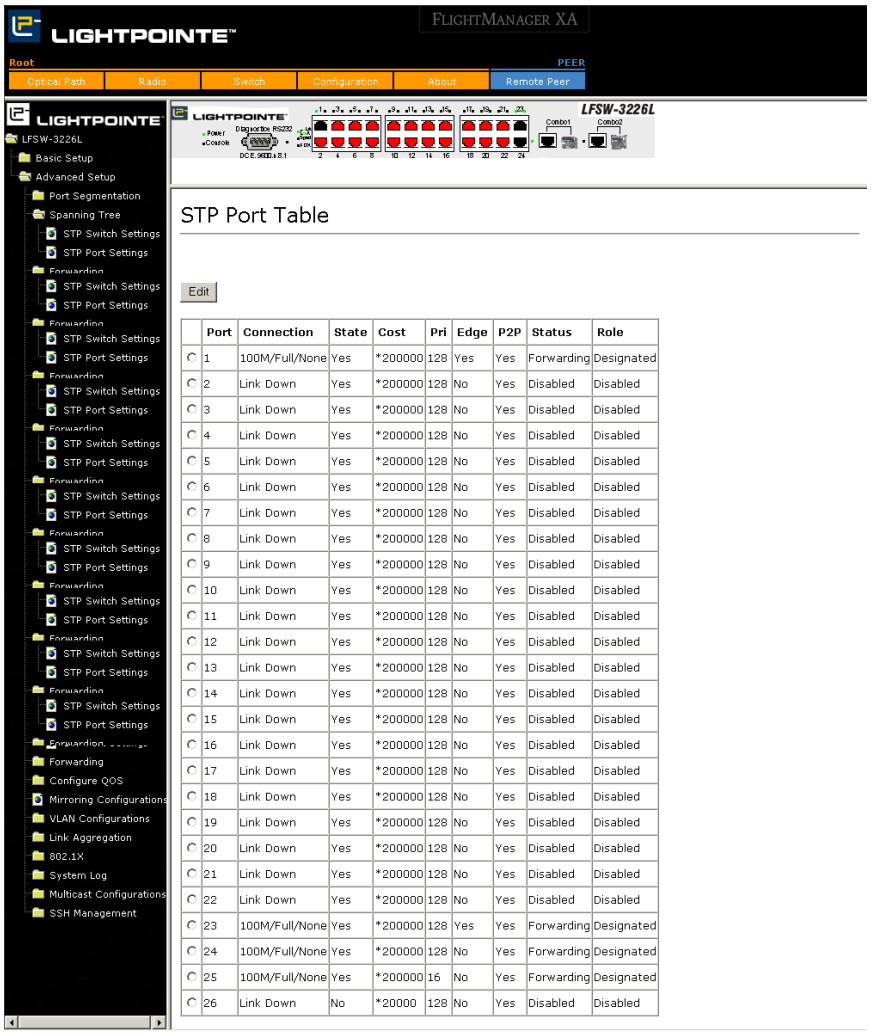
Step 10 Click the **STP Switch Settings** option. The STP Switch Settings window is displayed.



Use the factory default settings shown above.

- ❑ Local Priority set to 4096
- ❑ Peer Priority set to 8192

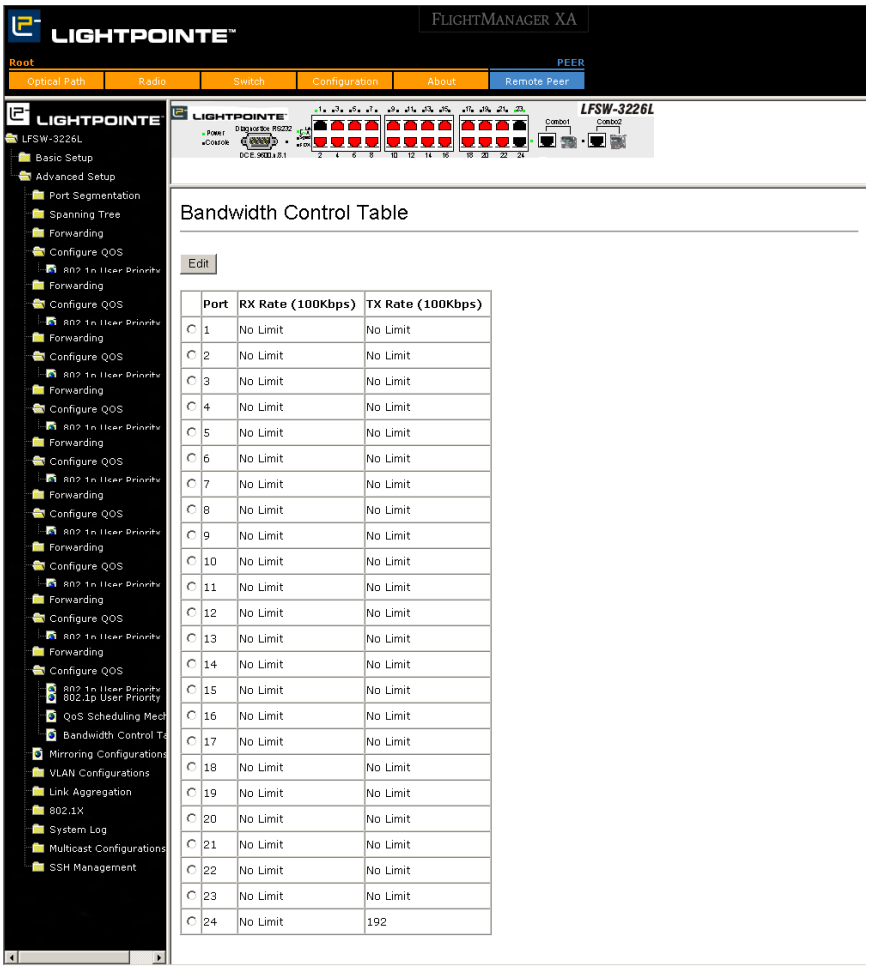
Step 11 Click the **STP Port Table** option. The STP Port Table window is displayed (example window shown, your settings may be different).



	Port	Connection	State	Cost	Pri	Edge	P2P	Status	Role
○	1	100M/Full/None	Yes	*200000	128	Yes	Yes	Forwarding	Designated
○	2	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	3	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	4	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	5	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	6	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	7	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	8	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	9	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	10	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	11	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	12	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	13	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	14	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	15	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	16	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	17	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	18	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	19	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	20	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	21	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	22	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	23	100M/Full/None	Yes	*200000	128	Yes	Yes	Forwarding	Designated
○	24	100M/Full/None	Yes	*200000	128	No	Yes	Forwarding	Designated
○	25	100M/Full/None	Yes	*200000	16	No	Yes	Forwarding	Designated
○	26	Link Down	No	*20000	128	No	Yes	Disabled	Disabled

Use the factory default settings of your system configuration.

Step 12 Click the **Bandwidth Control Table** option. The Bandwidth Control Table window is displayed.



	Port	RX Rate (100Kbps)	TX Rate (100Kbps)
○	1	No Limit	No Limit
○	2	No Limit	No Limit
○	3	No Limit	No Limit
○	4	No Limit	No Limit
○	5	No Limit	No Limit
○	6	No Limit	No Limit
○	7	No Limit	No Limit
○	8	No Limit	No Limit
○	9	No Limit	No Limit
○	10	No Limit	No Limit
○	11	No Limit	No Limit
○	12	No Limit	No Limit
○	13	No Limit	No Limit
○	14	No Limit	No Limit
○	15	No Limit	No Limit
○	16	No Limit	No Limit
○	17	No Limit	No Limit
○	18	No Limit	No Limit
○	19	No Limit	No Limit
○	20	No Limit	No Limit
○	21	No Limit	No Limit
○	22	No Limit	No Limit
○	23	No Limit	No Limit
○	24	No Limit	192

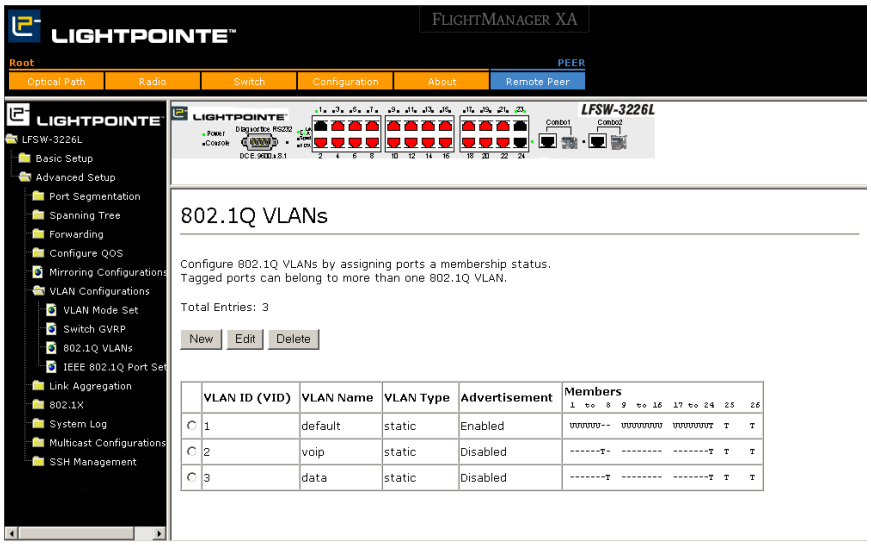
Use the factory default settings shown above.

- ❑ Port 24 TX Rate set to 192

Note: Any changes made to the Switch configuration during the current session must be saved. From the **Basic Setup** window, select the **Save Changes** window.

Step 13 Optional Step: Priority queuing of frame packet data.

Click the **VLAN Configuration** menu and select the **802.1 Q LANs** option. The 802.1 Q LANs window is displayed.



Ports 23 -26 are by default set as VLAN ports. The QoS (Quality of Service) The above screen is used to set up the Switch to utilize 802.1p priority queuing.

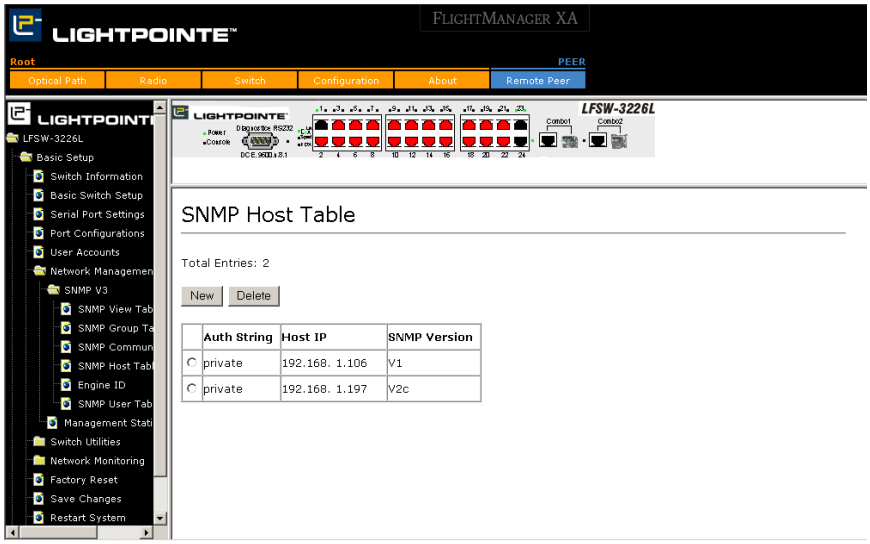
Note: The Switch default state is QoS On. The following settings are examples only. The actual settings are all customer network specific. The Local Switch is named "vlan"; the Peer is named "vlan1".

- ❑ Vlan on the Switch named "voip" created with ID of "2".
- ❑ vlan on the Switch named "data" created with ID of "3".
- ❑ Ports 24-26 added to the port list of a previously configured vlan "default"
- ❑ Ports 24-26 added to the port list of a previously configured vlan "voip".
- ❑ Ports 24-26 added to the port list of a previously configured vlan "data".

Note: Any changes made to the Switch configuration during the current session must be saved. From the **Basic Setup** window, select the **Save Changes** window.

Step 14 Optional Step: You can manage the Switch with an SNMP-compatible console program such as HP Openview. The Switch supports SNMP version 1, 2c and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch.

Click the **Network Management menu** and select the **SNMP Host Table** option. The SNMP Host Table window is displayed.



The following settings are examples only. The SNMP server in the following example has an IP address of 192.168.1.100. The actual SNMP server IP address is customer network specific.

- ❑ Enable SNMP traps
- ❑ Create a host recipient of SNMP traps generated by the Switch's SNMP, set the SNMP version to v1 OR v2c, and specify packet authorization and encryption.

Note: Any changes made to the Switch configuration during the current session must be saved. From the **Basic Setup** window, select the **Save Changes** window.

Step 15 To configure the Peer Switch, repeat steps 4 through 15.


LIGHTPOINTE™

3. Overview of Basic Switch Settings

This chapter contains a detailed discussion about viewing and configuring some of the basic functions of the switch, including:

- Switch Information
- Basic Switch Setup
- Serial Port Setting
- Port Configurations
- User Accounts
- Network Management
- Switch Utilities
- Network Monitoring
- Factory Reset
- Save Changes
- Restart System
- Logout

NOTE: The LFSW-3226L switch has been customized and pre-configured to ensure optimal performance in LightPointe optical wireless installations. Any changes to default settings or use of advanced switch features may impact the operation of the optical wireless link.

3.1. Introduction

All software function of the LFSW-3226L Switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser.

The following subsections review how to change some of the basic settings for the Switch such as changing IP settings and assigning user names and passwords for management access privileges, as well as how to save the changes and restart the Switch.

3.2. Switch Information

Click the **Switch Information** link in the Configuration menu.

Switch Information

Displays information about the switch's hardware and firmware.

Device Type	LFSW-3226L Fast-Ethernet Switch
MAC Address	00-01-02-03-04-05
Get IP From	Manual
IP Address	10.53.13.4
VLAN Name	default
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
Boot PROM Version	Build 00.00.11
Firmware Version	Build 2.0.32
Hardware Version	-
Name	
Location	
Contact	
Spanning Tree	Disabled
GVRP	Disabled
IGMP Snooping	Disabled
SSH	Enabled (TCP 22)
TELNET	Enabled (TCP 23)
WEB	Enabled (TCP 80)
RMON	Disabled

Figure 3-1: Switch Information – Basic Settings window

The **Switch Information** window shows the Switch's **MAC Address** (assigned by the factory and unchangeable), IP configuration and some important functions implemented and their status. In addition, the **Boot PROM** and **Firmware Version** numbers are shown. This information is helpful to keep track of PROM and Firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary.

3.3. Basic Switch Setup

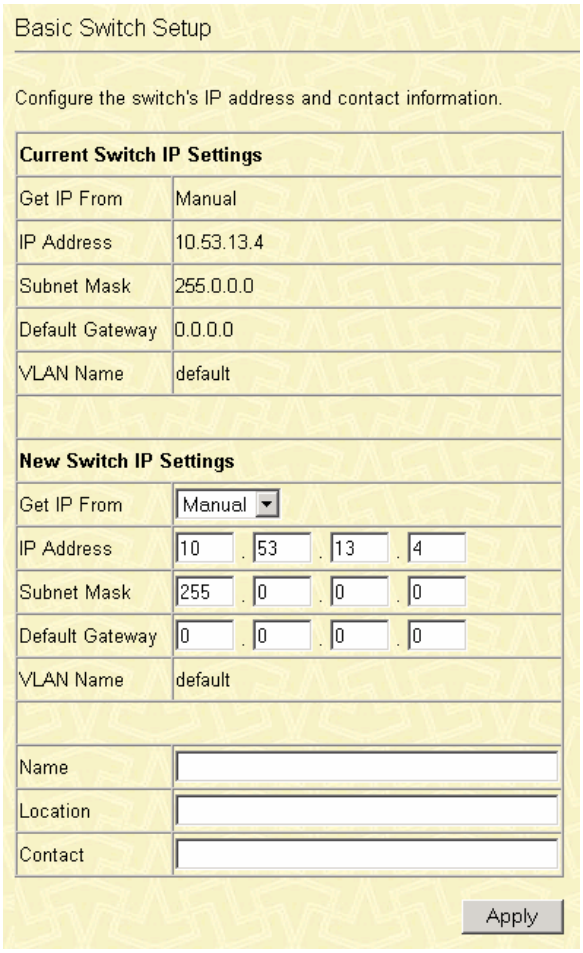
The **Basic Switch Setup** may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the Introduction of the CLI Reference or skip ahead to the end of this section for a quick description of how to use the console port and CLI IP settings commands to establish IP settings for the Switch.

To change IP settings using the web manager you must access the **Basic Switch Setup** menu located in the **Management** folder.

To configure the switch's IP address:

To manually assign the switch's IP address, subnet mask, and default gateway address:

Step 1 Open the Management folder and click the Basic Switch Settings menu button. The web manager will display the Switch's current IP settings and an IP configuration menu, as seen below.



Step 2 To manually assign the switch's IP address, subnet mask, and default gateway address:

- Select **Manual** from the **Get IP From** drop-down menu.
- Enter the appropriate IP address and subnet mask.
- If you want to access the switch from a different subnet from the one it is installed on, enter the IP address of the gateway. If you will manage the switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.
- If no VLANs have been previously configured on the switch, you can use the default VLAN Name (default). The default VLAN contains all of the switch ports as members. If VLANs have been previously configured on the Switch, you will need to enter the VLAN ID of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.

Step 3 To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address:

- Use the Get IP From: pull-down menu to choose from BOOTP or DHCP. This selects how the Switch will be assigned an IP address on the next reboot.

The Basic Switch Setup options are:

Table 3-1: Basic Switch Setup Options

Parameter	Description
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
Manual	Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields which require entries under this option are as follows:
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Default Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

Parameter	Description
VID	This allows the entry of a VLAN ID from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one entered in the VID field will not be able to manage the Switch in-band unless their IP addresses are entered in the Security IP Management menu. If VLANs have not yet been configured for the Switch, the default VID (1) contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until either a management VLAN is specified or Management Station IP Addresses are assigned.

3.4. Serial Port Settings

The **Serial Port Settings** window may be found in the **Basic Setup** folder. This window is used to configure the console settings for the Command Line Interface or for a Telnet session.

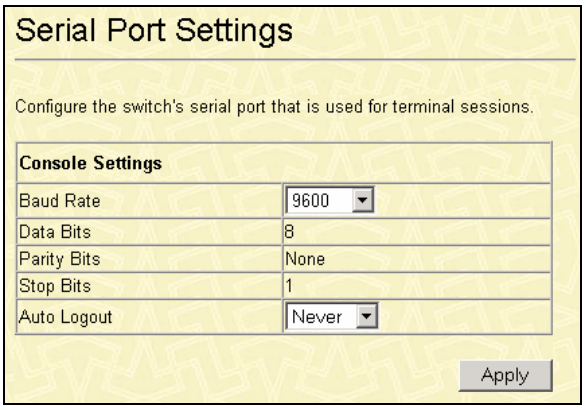
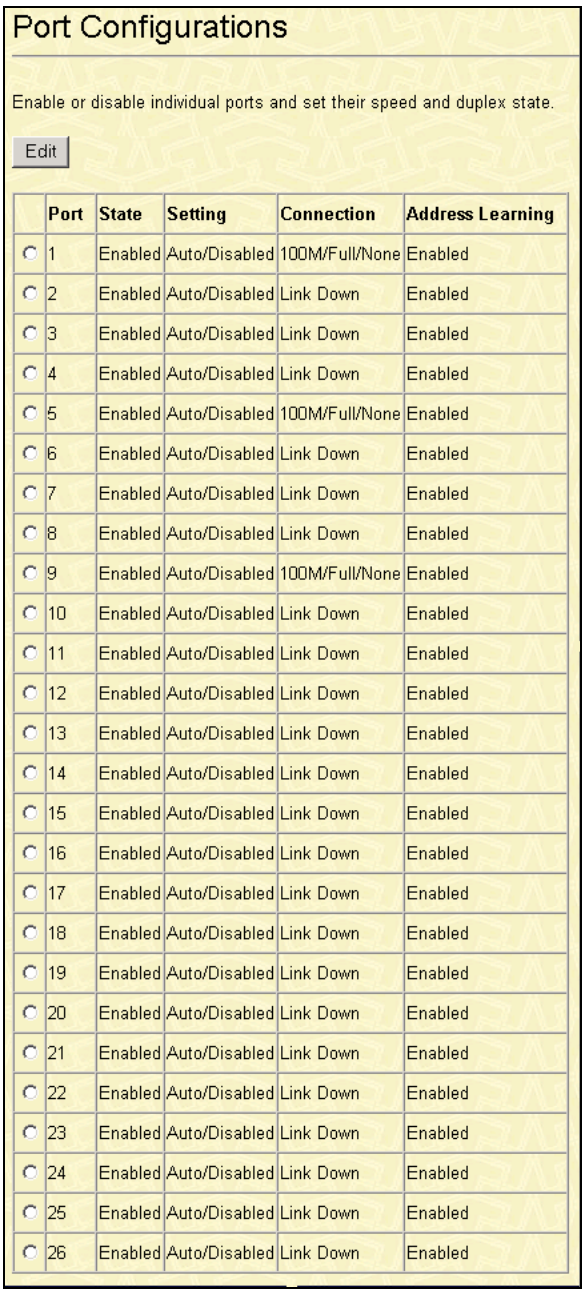


Figure 3-2: Serial Port Settings window

The **Serial Port Settings** window is used to change and view the Console settings for your switch. The default **Baud Rate** for this switch is set at 9600 and may be altered from 119200, 38400, to 115200 to perform different functions. **Data Bits**, **Parity Bits** and **Stop Bits** are read only fields and cannot be changed using the web-based manager. The **Auto Logout** field may be set to Never, 2 minutes, 5 minutes, 10 minutes, and 15 minutes**,** depending on the time the user wishes the Switch to be idle before automatically logging out. The default for this setting is 10 minutes.

3.5. Port Configurations

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control. Clicking on **Port Configurations** will open the following window for the user.



	Port	State	Setting	Connection	Address Learning
○	1	Enabled	Auto/Disabled	100M/Full/None	Enabled
○	2	Enabled	Auto/Disabled	Link Down	Enabled
○	3	Enabled	Auto/Disabled	Link Down	Enabled
○	4	Enabled	Auto/Disabled	Link Down	Enabled
○	5	Enabled	Auto/Disabled	100M/Full/None	Enabled
○	6	Enabled	Auto/Disabled	Link Down	Enabled
○	7	Enabled	Auto/Disabled	Link Down	Enabled
○	8	Enabled	Auto/Disabled	Link Down	Enabled
○	9	Enabled	Auto/Disabled	100M/Full/None	Enabled
○	10	Enabled	Auto/Disabled	Link Down	Enabled
○	11	Enabled	Auto/Disabled	Link Down	Enabled
○	12	Enabled	Auto/Disabled	Link Down	Enabled
○	13	Enabled	Auto/Disabled	Link Down	Enabled
○	14	Enabled	Auto/Disabled	Link Down	Enabled
○	15	Enabled	Auto/Disabled	Link Down	Enabled
○	16	Enabled	Auto/Disabled	Link Down	Enabled
○	17	Enabled	Auto/Disabled	Link Down	Enabled
○	18	Enabled	Auto/Disabled	Link Down	Enabled
○	19	Enabled	Auto/Disabled	Link Down	Enabled
○	20	Enabled	Auto/Disabled	Link Down	Enabled
○	21	Enabled	Auto/Disabled	Link Down	Enabled
○	22	Enabled	Auto/Disabled	Link Down	Enabled
○	23	Enabled	Auto/Disabled	Link Down	Enabled
○	24	Enabled	Auto/Disabled	Link Down	Enabled
○	25	Enabled	Auto/Disabled	Link Down	Enabled
○	26	Enabled	Auto/Disabled	Link Down	Enabled

Figure 3-3: Port Configurations window

To edit a specific port's settings, click the corresponding radio button of the port and click **Edit**, which will reveal menu below.

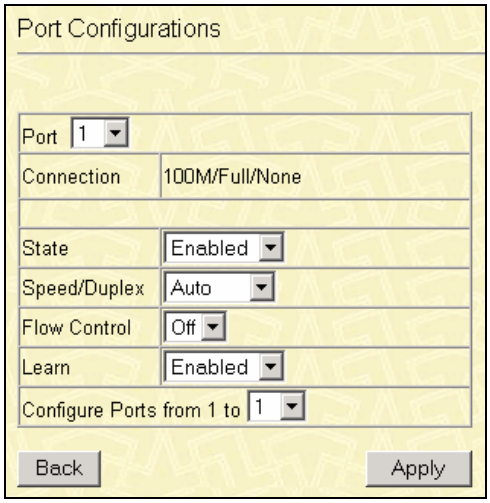


Figure 3-4: Port Configurations – Edit window

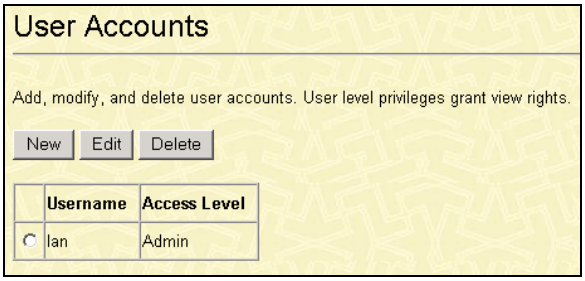
Note: The user may also choose a port to configure by selecting a port on the Switch's front panel at the top of the web-based user interface page.

This window allows the user to set the following fields:

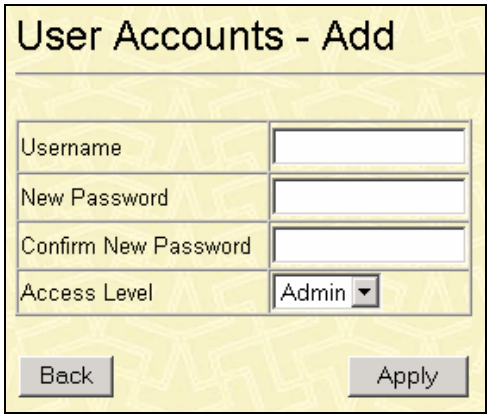
Field	Description
Connection	Displays the current uplink status of the specified port.
State	The user may enable or disable the port by choosing the appropriate option from the pull down menu.
Speed/Duplex	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. Auto – auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. ❑ The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. ❑ The other options are 100M/Full, 100M/Half, 10M/Full and 10M/Half. There is no automatic adjustment of port settings with any option other than Auto. ❑ For the two Mini-GBIC Combo ports, the user may set the speed to Auto, 100M/Full, 100M/Half, 10M/Full and 10M/Half for the copper ports. Using the fiber-optic ports, the user may set speeds of 1000M/Full and Auto.
Flow Control	Enables or disables the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two. The default is On.
Learn	Enable or disable MAC address learning for the selected ports. When Enabled, destination and source MAC addresses are automatically listed in the forwarding table. When learning is Disabled, the switch will be unable to learn new MAC addresses.
Configure Ports from	The user may set the same port configurations for multiple ports by using this option. The ports may only be chosen in block, commencing with the port initially chosen by the user to configure. The user may use the pull down menu to specify the end port of the block of ports.

3.6. User Accounts

Step 1 From the **Basic Setup** menu, click **User Accounts** and the following window appears.



Step 2 Click **New** to add a new user account, utilizing the window below.



- Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have Admin or User privileges.
- Click **Apply** to make the user addition effective.
- A listing of all user accounts and access levels is shown in the **User Account Management** window. This list is updated when Apply is executed. Click **Show All User Account Entries** to access this window.
- Please remember that Apply makes changes to the switch configuration for the **current session only**. All changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the **Main Menu** - if you want these changes to be permanent.

Step 3 To edit a User Account, click the radio button of the corresponding User Account and click **Edit**. To delete a User Account, click the radio button of the corresponding User Account and click **Delete**.

3.6.1. Admin and User Privileges

There are two levels of user privileges: Admin and User. Some menu selections available to users with Admin privileges may not be available to those with User privileges.

The following table summarizes the Admin and User privileges:

Table 3-2: Admin and User Privileges

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

After establishing a User Account with Admin-level privileges, go to the **Maintenance** menu and click **Save Changes**. Next click **Save Configuration**. The switch will now save any changes to its non-volatile ram and reboot. You can logon again and are now ready to continue configuring the Switch.

3.7. Network Management

The LFSW-3226L allows you to manage the switch via the **Network Management** menu. This switch uses SNMPv3 for management purposes, as seen below.

3.7.1. SNMPv3

The LFSW-3226L incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The LFSW-3226L supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP View Table

The **SNMP View Table** is used to assign views to community strings that define which MIB objects can be accessed by an SNMP manager. To access the view table, click **Basic Setup** > **Network Management** > **SNMP V3** > **SNMP View Table**.

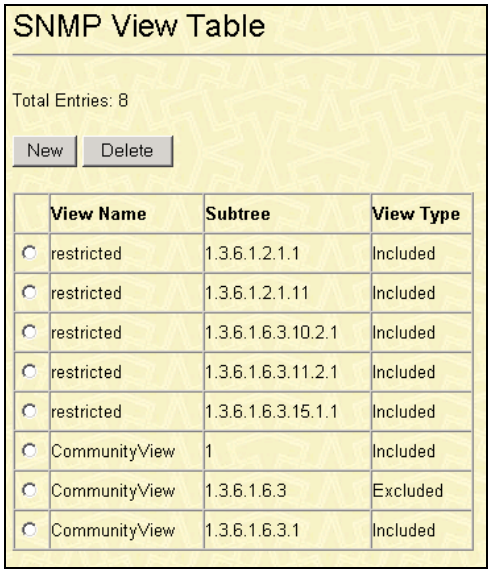


Figure 3-5: SNMP View Table

To delete an existing **SNMP View Table** entry, click the selection button on the far left that corresponds to the port you want to configure and click the **Delete** button. To create a new entry, click the **New** button, and a separate menu will appear.

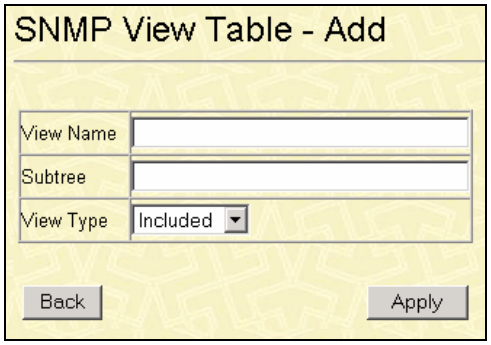


Figure 3-6: SNMP View Table – Add window

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

The following parameters can be set:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select Included to include this object in the list of objects that an SNMP manager can access. Select Excluded to exclude this object from the list of objects that an SNMP manager can access.

SNMP Group Table

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

To view the group table, click Basic Setup > Network Management > SNMP V3 > Group Table.

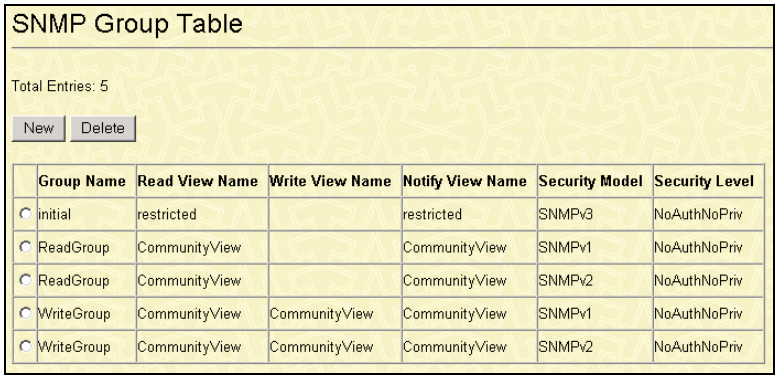


Figure 3-7: SNMP Group Table window

To delete an existing **SNMP Group Table** entry, click the corresponding radio button and click **Delete**.

To add a new entry to the Switch's **SNMP Group Table**, click the **New** button in the upper left-hand corner of the **SNMP Group Table** page. This will open the **SNMP Group Table - Add** page, as shown below.

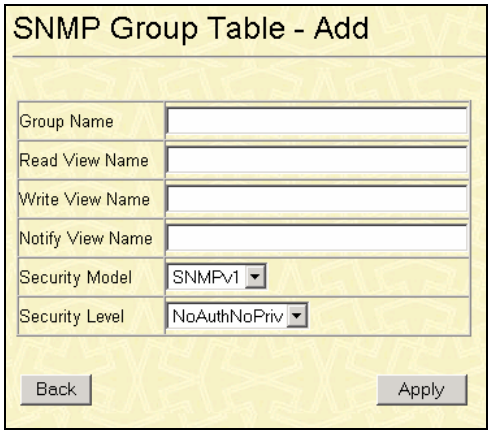


Figure 3-8: SNMP Group Table – Add window

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created that can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
Security Model	SNMPv1 – Specifies that SNMP version 1 will be used. SNMPv2 – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. SNMPv3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Security Level	NoAuthNoPriv – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. AuthNoPriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. AuthPriv – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

SNMP Community Table

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

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

To view the community table, click Basic Setup > Network Management > SNMP V3 > SNMP Community Table.

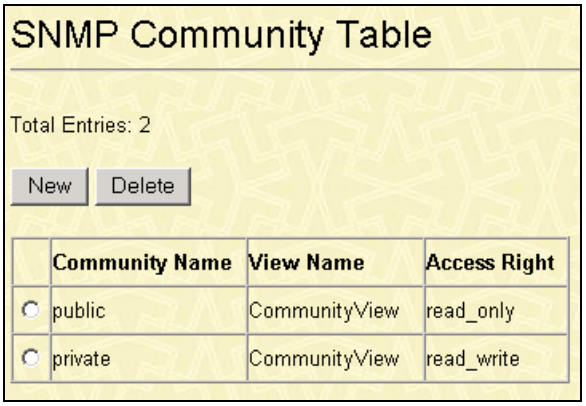


Figure 3-9: SNMP Community Table window

To delete an existing entry, click the corresponding radio button and then click the **Delete** button. To add a new entry to the **SNMP Community Table**, click **New** to access the following screen.

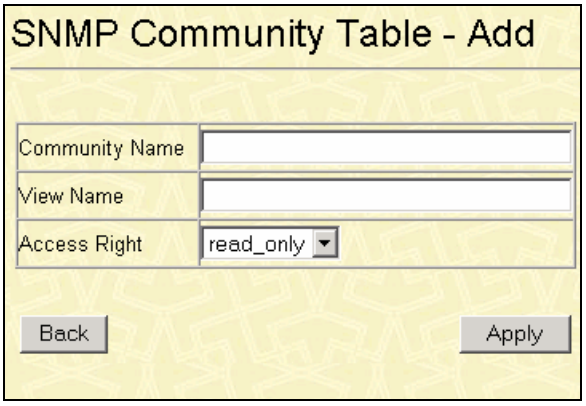


Figure 3-10: SNMP Community Table – Add window

The following parameters can be set:

Parameter	Description
Community Name	Type an alphanumeric string of up to 33 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	read_only – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. read_write – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch.

SNMP Host Table

Use the **SNMP Host Table** to set up SNMP trap recipients.

Open the **Basic Setup** folder to **Network Management,** and then the **SNMPV3** folder. Finally, click on the **SNMP Host Table** link. This will open the **SNMP Host Table** page, as shown below.

To delete an existing SNMP Host Table entry, click the corresponding radio button entry and then the **Delete** button.

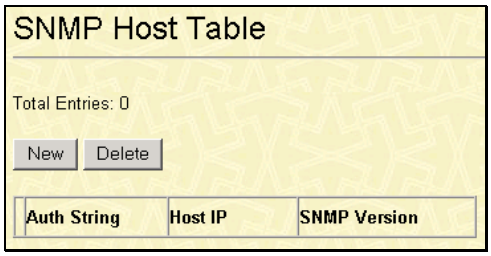


Figure 3-11: SNMP Host Table window

To add a new entry to the switch's SNMP Group Table, click the **New** button in the upper left-hand corner of the **SNMP Host Table** page. This will open the **SNMP Host Table - Add** page, as shown below.

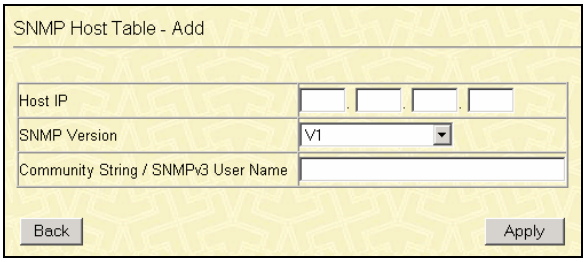


Figure 3-12: SNMP Host Table – Add window

The following parameters can be set:

Parameter	Description
IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	V1 – To specify that SNMP version 1 will be used. V2c – To specify that SNMP V2c version will be used. V3 – NoAuth –NoPriv – To specify that SNMP version 3 will be used, with the NoAuth-NoPriv security level. V3 – Auth - NoPriv -To specify that the SNMP version 3 will be used, with the Auth-NoPriv security level. V3 – Auth - Priv -To specify that the SNMP version 3 will be used, with the Auth-Priv security level.
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

SNMP Engine ID

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

To display the switch's SNMP Engine ID, open the **Basic Setup** folder to **Network Management**, and then the **SNMPV3** folder. Finally, click on the **Engine ID** link. This will open the **SNMP Engine ID** Configuration page, as shown below.

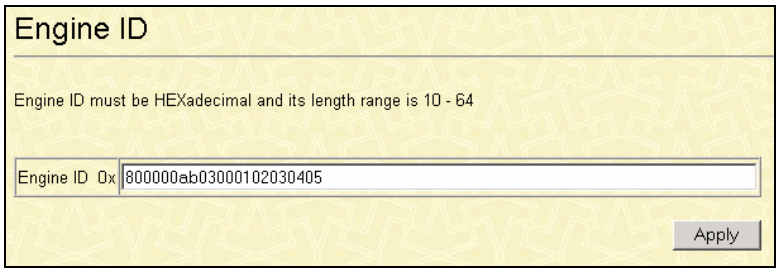


Figure 3-13: Engine ID window

To change the **Engine ID**, type the new **Engine ID** in the space provided and click the **Apply** button.

SNMP User Table

The SNMP User Table displays all of the SNMP User's currently configured on the Switch.

Open the **Basic Setup** folder and then the N**etwork Management** folder. Click on **SNMPV3** and finally click on the **SNMP User Table** link. This will open the **SNMP User Table**, as shown below.

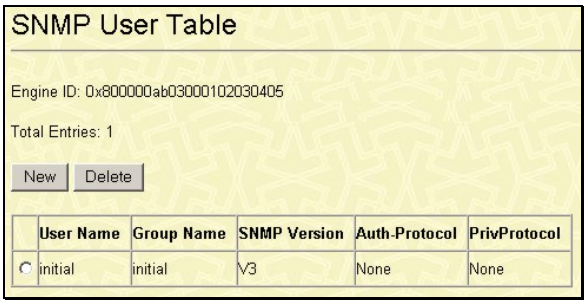


Figure 3-14: SNMP User Table window

To delete an existing entry, click the corresponding radio button and then click the **Delete** button. To add a new entry to the **SNMP Community Table**, click **New** to access the following window.

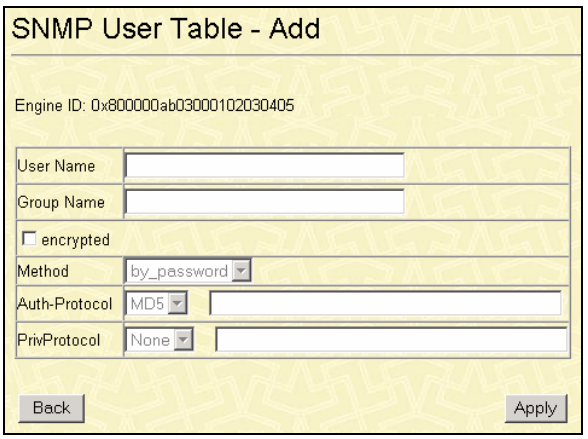


Figure 3-15: SNMP User Table – Add window

The following parameters can be set:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created that can request SNMP messages.

Parameter	Description
encrypted	Checking the corresponding box will enable encryption for SNMP V3 and is only operable in SNMP V3 mode. This will also make the Method, Auth-Protocol and PrivProtocol parameters operable.
Method	The user may choose between by_password and by_key for the method of encryption used for the SNMP function.
Auth-Protocol	None – Indicates that no authorization protocol is in use. MD5 – Indicates that the HMAC-MD5-96 authentication level will be used. SHA – Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol	None – Indicates that no authorization protocol is in use. DES – Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

3.7.2. Management Station IP Addresses

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

To view and configure the **Management Station IP** window, open the **Basic Setup** folder, then click **Network Management** > **Management Station IP Addresses**, which opens the following screen.

Figure 3-16: Management Station IP Addresses window

3.8. Switch Utilities

The **Switch Utilities** menu will aid the user in maintaining some of the basic utilities of the switch, such as TFTP services and the Ping test. See below for further description.

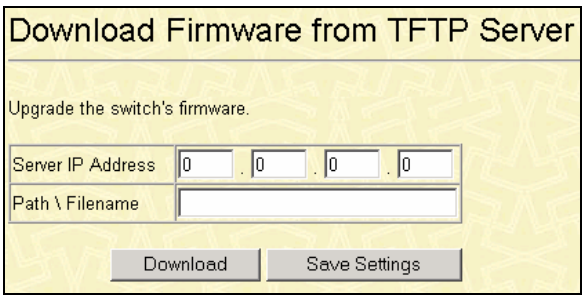
3.8.1. TFTP Services

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

Download Firmware from TFTP Server

Figure 5 - 1. Download Firmware from TFTP Server window

Step 1 To update the Switch's firmware, click Basic Setup > TFTP Services > Download Firmware from TFTP Server. The following screen is displayed.



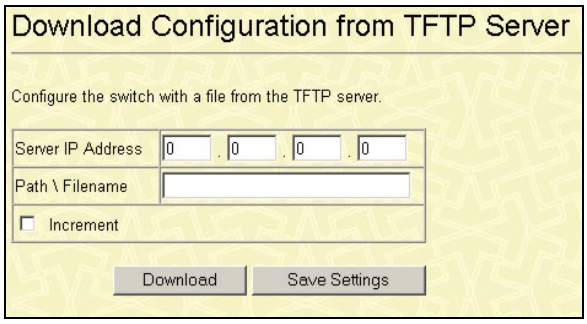
Step 2 Enter the full location of the firmware in the **Path/Filename** field.

Step 3 Click **Save Settings** to record the IP address of the TFTP server.

Step 4 Click **Download** to initiate the file transfer.

Download Configuration File

Step 1 To download a configuration file from a TFTP server, click **Basic Setup** > **Switch Utilities > TFTP Services** > **Download Configuration File from TFTP Server** link to access the following window.



Step 2 Enter the IP address of the TFTP server and specify the location of the Switch configuration file on the TFTP server.

Step 3 Enter the full location of the firmware in the Path/Filename field.

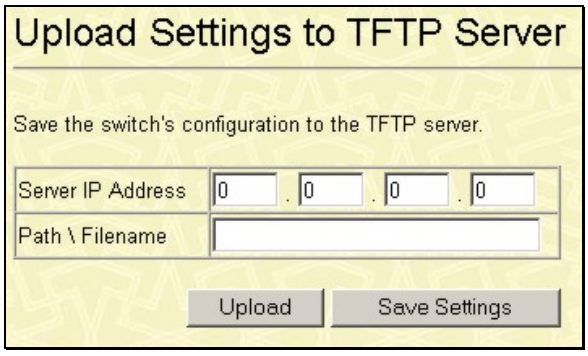
Step 4 Clicking the Increment box will allow the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.

Step 5 Click Save Settings to record the IP address of the TFTP server.

Step 6 Click Download to initiate the file transfer.

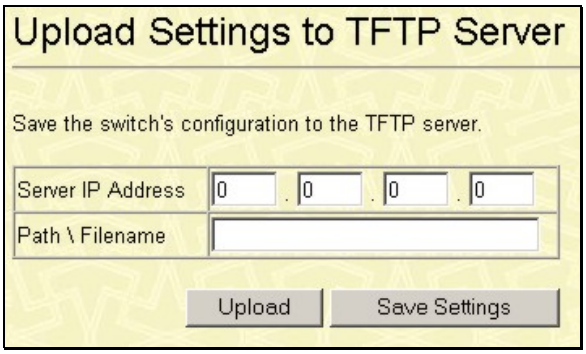
Download/Upload Settings to TFTP Server

Step 1 To download a configuration file for the Switch, click on the **Switch Utilities** > **TFTP Services** > **Upload Settings to TFTP Server** link



Step 2 Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server and click **Upload** to initiate the file transfer. Click **Save Settings** to record the IP address of the TFTP server

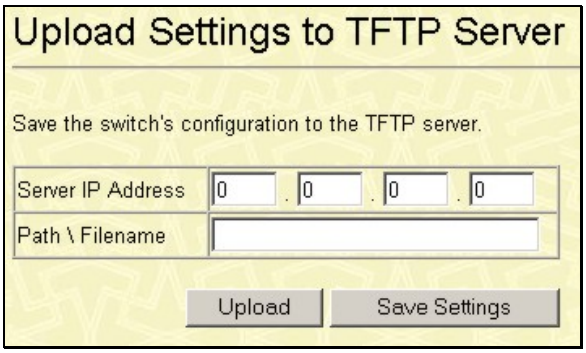
Step 3 To download a configuration file for the Switch, click on the **Switch Utilities** > **TFTP Services** > **Upload Settings to TFTP Server** link.



Step 4 Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server and click **Upload** to initiate the file transfer.

Step 5 Click **Save Settings** to record the IP address of the TFTP server

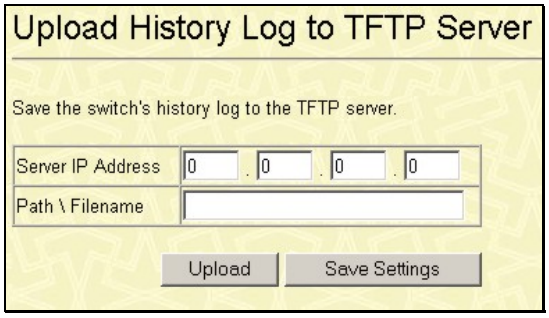
Step 6 To download a configuration file for the Switch, click on the **Switch Utilities** > **TFTP Services** > **Upload Settings to TFTP Server** link.



Step 7 Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server and click Upload to initiate the file transfer. Click Save Settings to record the IP address of the TFTP server

Upload History Log to TFTP Server

Step 1 To upload the Switch history log file to a TFTP server, click on the **Switch Utilities** > **TFTP Services** > **Upload History Log to TFTP Server** link.



Step 2 Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. Click **Apply** to make the changes current.

Step 3 Click **Upload** to initiate the file transfer

3.8.2. Ping Test

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

To access the Ping program, click Basic Setup> Switch Utilities > Others > Ping Test.

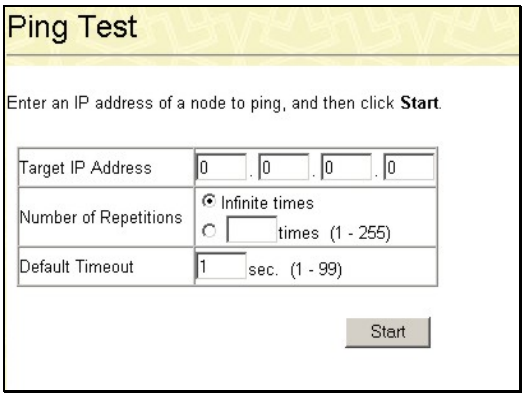


Figure 3-17: Ping Test window

The **Infinite times** checkbox, in the **Number of Repetitions** section, tells PING to keep sending data packets to the specified IP address until the program is stopped. The **Default Timeout** field may be set from 1 to 99 seconds. This is the time that the Switch limits the Ping Test to continue pinging.

3.9. Network Monitoring

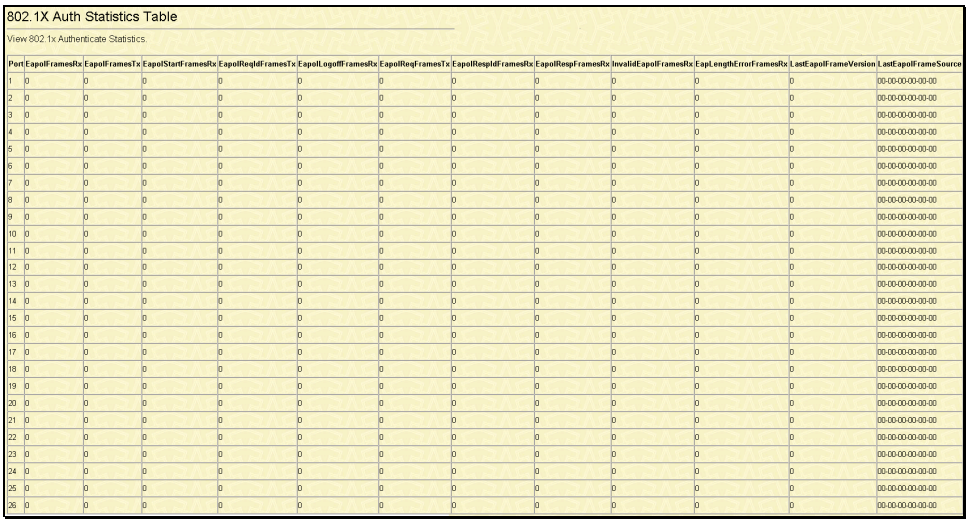
The LFSW-3226L provides network monitoring capabilities that can be viewed under the **Network Monitoring** menu in the **Basic Setup** folder. The menu consists of windows showing port statistics, address tables and the current switch status. See below for further description.

3.9.1. 802.1X

The 802.1X window consists of 802.1X Auth Statistics, 802.1X Auth Session, 802.1X Auth Client, and 802.1X Diagnostics.

802.1X Auth Statistics

This is a read-only field is used to display the authenticator statistics information on the switch. To view this window, click Basic Setup > Network Monitoring > 802.1X Auth Statistics.



802.1X Auth Statistics Table

View 802.1x Authenticate Statistics.

Port	EapolFramesRx	EapolFramesTx	EapolStartFramesRx	EapolReqIdFramesTx	EapolLogoffFramesRx	EapolReqFramesTx	EapolRespIdFramesRx	EapolRespFramesRx	InvalidEapolFramesRx	EapLengthErrorFramesRx	LastEapolFrameVersion	LastEapolFrameSource
1	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
2	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
3	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
4	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
5	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
6	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
7	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
8	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
9	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
10	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
11	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
12	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
13	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
14	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
15	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
16	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
17	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
18	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
19	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
20	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
21	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
22	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
23	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
24	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
25	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00
26	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00-00

Figure 3-18: 802.1X Auth Statistics Table window

802.1X Auth Session

This is a read-only field is used to display the authenticator statistics information on the switch. To view this window, click **Basic Setup > Network Monitoring > 802.1X Auth Session**.

802.1X Auth Session Statistics

View 802.1x Authenticate Session.

Port	SessionOctetsRx	SessionOctetsTx	SessionFramesRx	SessionFramesTx	SessionId	SessionAuthenticMethod	SessionTime	SessionTerminateCause	SessionUserName
1	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
2	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
3	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
4	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
5	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
6	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
7	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
8	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
9	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
10	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
11	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
12	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
13	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
14	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
15	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
16	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
17	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
18	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
19	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
20	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
21	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
22	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
23	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
24	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
25	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	
26	0	0	0	0		Remote Authentication Server	0	SupplicantLogoff	

Figure 3-19: 802.1X Auth Session Statistics window

802.1X Auth Client

This is a read-only field is used to display the RADIUS Auth Client information on the switch. To view this window, click **Basic Setup > Network Monitoring > 802.1X Auth Client**.

Radius Auth Client Table

View Radius Authenticate Client.

radiusAuthClientInvalidServerAddresses	radiusAuthClientIdentifier	radiusAuthServerIndex	radiusAuthServerAddress	radiusAuthClientServerPortNumb
0	D-Link	1	0.0.0.0	0
0	D-Link	2	0.0.0.0	0
0	D-Link	3	0.0.0.0	0

Figure 3-20: RADIUS Auth Client Table window

802.1X Auth Diagnostics

This is a read-only field is used to display the authenticator diagnostics information on the switch. To view this window, click **Basic Setup > Network Monitoring > 802.1X Diagnostics**.

Figure 3-21: 802.1X Auth Diagnostics Table window

802.1X Accounting Client

This is a read-only field is used to display the RADIUS Accounting information on the switch. To view this window, click **Basic Setup > Network Monitoring > 802.1X Accounting Client**.

Radius Auth Client Table

View Radius Authenticate Client.

radiusAuthClientInvalidServerAddresses	radiusAuthClientIdentifier	radiusAuthServerIndex	radiusAuthServerAddress	radiusAuthClientServerPortNumb
0	LightPointe	1	0.0.0.0	0
0	LightPointe	2	0.0.0.0	0
0	LightPointe	3	0.0.0.0	0

Figure 3-22: RADIUS Accounting Client Table window

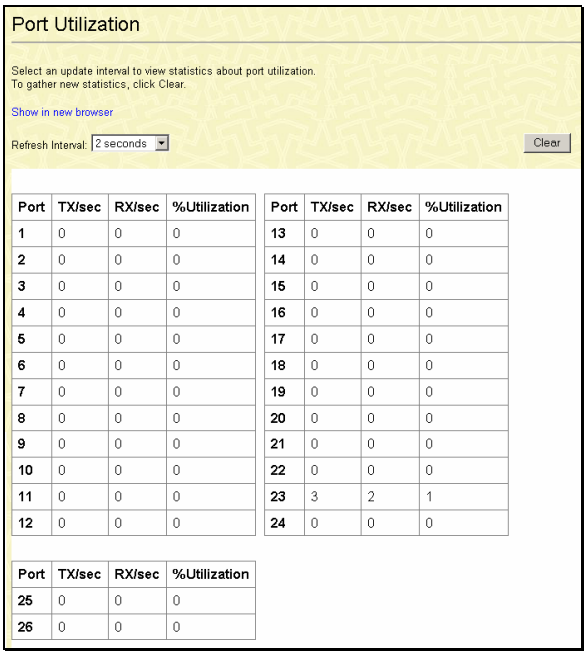
3.9.2. Statistics

The Statistics windows consist of Port Utilization, Port Error Packets, and Port Packet Analysis.

Port Utilization

The Port Utilization window displays the percentage of the total available bandwidth being used on the port. Port Utilization statistics may be viewed using the table format.

To view the port utilization, click Basic Setup > Network Monitoring > Statistics > Port Utilization:



Port	TX/sec	RX/sec	%Utilization
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0

Port	TX/sec	RX/sec	%Utilization
13	0	0	0
14	0	0	0
15	0	0	0
16	0	0	0
17	0	0	0
18	0	0	0
19	0	0	0
20	0	0	0
21	0	0	0
22	0	0	0
23	3	2	1
24	0	0	0

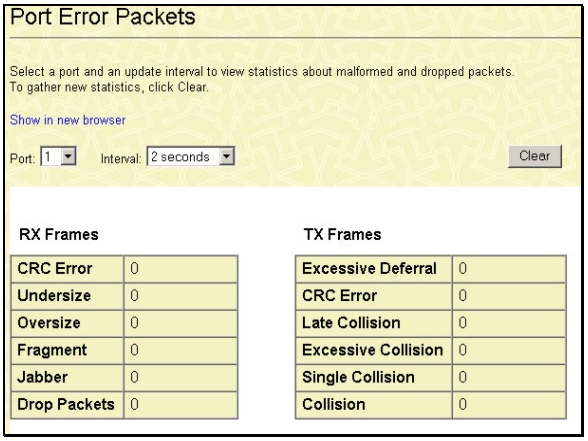
Port	TX/sec	RX/sec	%Utilization
25	0	0	0
26	0	0	0

Figure 3-23: Port Utilization window

To clear the current port utilization statistics, click **Clear**. The window will automatically refresh with new updated statistics. If the user wishes to view these statistics in a separate window from the web-based management, click **Show in new browser**. The time between updates received from the switch may be chosen by using the pull-down menu of the **Refresh Interval** field. The user may choose intervals of 2, 5, 15, 30 and 60 seconds Suspend will stop the updates. The default setting for this field is 2 seconds.

Port Error Packets

The **Port Error Packets** window shows the number and type of error packets received by the switch. To view the **Port Error Packets** windows, click **Basic Setup > Network Monitoring > Statistics > Port Error Packets**.



CRC Error	0
Undersize	0
Oversize	0
Fragment	0
Jabber	0
Drop Packets	0

Excessive Deferral	0
CRC Error	0
Late Collision	0
Excessive Collision	0
Single Collision	0
Collision	0

Figure 3-24: Port Error Packets window

Select the desired port using the **Port** drop-down menu. The **Interval** field sets the interval at which the error statistics are updated. The user may choose intervals of 2, 5, 15, 30 and 60 seconds. Suspend will stop the updates. The default setting for this field is 2 seconds. If the user wishes to view these statistics in a separate window from the web-based management, click **Show in new browser**.

The following fields are displayed:

TX (transmit)

Parameter	Description
CRC Error	Counts otherwise valid frames that did not end on a byte (octet) boundary.
Undersize	The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
Oversize	Counts packets received that were longer than 1518 octets, or if a VLAN frame 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	The number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
Drop Packets	The number of frames that are dropped by this port since the last Switch reboot.

RX (receive)

Parameter	Description
Excessive Deferral	The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid frames that did not end on a byte (octet) boundary.
Late Collision	Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collision	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.
Single Collision	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.

Port Packet Analysis

The Web Manager allows packets received by the Switch, arranged in groups, to be viewed as a table, as shown below.

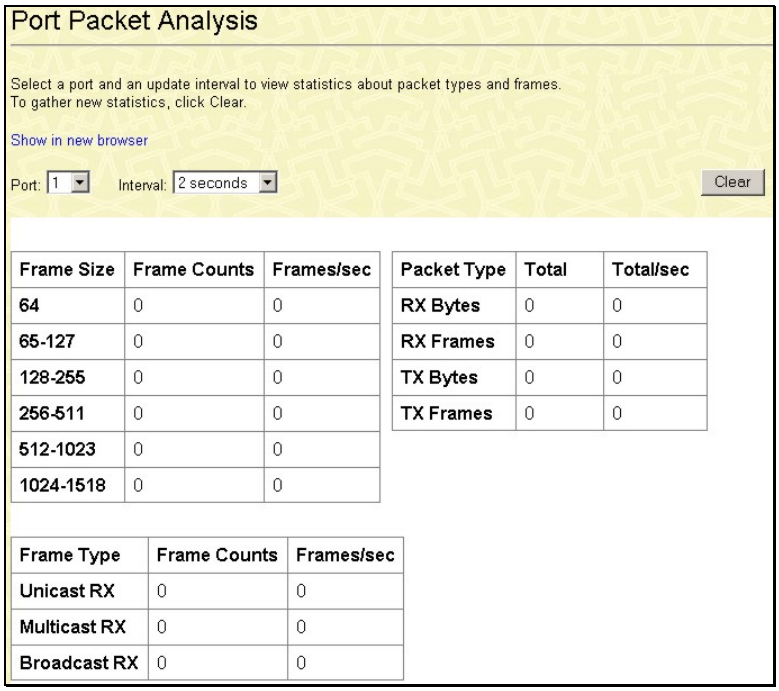


Figure 3-25: Port Packet Analysis window

Select the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated. The user may choose intervals of **2, 5, 15, 30** and **60** seconds. **Suspend** will stop the updates. The default setting for this field is **2 seconds**. If the user wishes to view these statistics in a separate window from the web-based management, click **Show in new browser**.

The results are separated into three tables, labeled **A**, **B**, and **C** in the window above. Table **A** is relevant to the size of the packets, Table **B** is relevant to the type of packets and Table **C** is relevant to the type of frame associated with these packets.

Table A: Size

Frame Size	Description
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Frame Size	Description
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1508	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Table B: Packet Type

Packet Type	Description
RX Bytes	Displays the number of bytes (octets) received by the Switch in total number (Total), and rate (Total/sec).
RX Frames	Displays the number of packets (frames) received by the Switch in total number (Total), and rate (Total/sec).
TX Bytes	Displays the number of bytes (octets) transmitted by the Switch in total number (Total), and rate (Total/sec).
TX Frames	Displays the number of packets (frames) transmitted by the Switch in total number (Total), and rate (Total/sec).

Table C: Frame Type

Frame Type	Description
Unicast RX	Displays the number of unicast packets received by the Switch in total number (Frames) and the rate (Frames/sec).
Multicast RX	Displays the number of multicast packets received by the Switch in total number (Frames) and the rate (Frames/sec).
Broadcast RX	Displays the number of broadcast packets received by the Switch in total number (Frames) and the rate (Frames/sec).

3.9.3. Address Tables

The Address Table window includes **MAC Address Tables**.

MAC Address Table

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

To view the MAC Address Table, click Basic Setup > Network Monitoring > Address Tables > MAC Address Table.

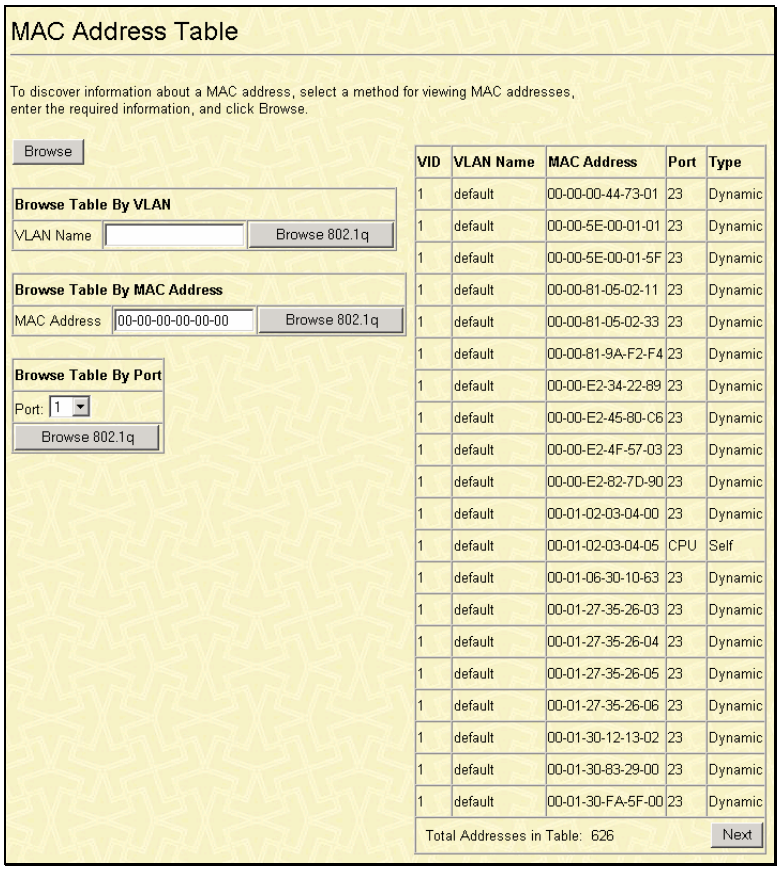


Figure 3-26: MAC Address Table window

The following fields can be set:

Parameter	Description
Browse Table By VLAN	Enter a VLAN name for the forwarding table to be browsed by and then click the Browse button.
Browse Table By MAC Address	Enter a MAC address for the forwarding table to be browsed by and then click the Browse button.
Browse Table By Port	Choose a port number for the forwarding table to be browsed by and then click the Browse button.

The following fields can be viewed in the table to the right.

Parameter	Description
VID	The VLAN ID number.
VLAN Name	The VLAN name.
MAC Address	The MAC address entered into the address table.
Port	The port that the MAC address above corresponds to.
Type	How the switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.

3.9.4. Status

The Status windows include GVRP Status, Router Ports, IGMP Snooping Group Table, and Switch History.

GVRP Status

This allows the GVRP status for each of the switch's ports to be viewed by the VLAN. This window displays the ports on the switch that are currently Egress or Untagged ports.

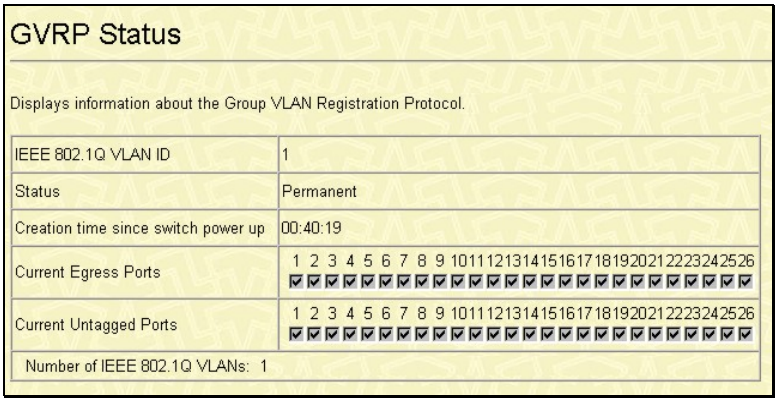


Figure 3-27: GVRP Status window

Router Ports

This displays which of the switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by **S**. A router port that is dynamically configured by the switch is designated by **D**.

To view the Router Ports table, click Basic Setup > Network Monitoring > Status > Router Ports:

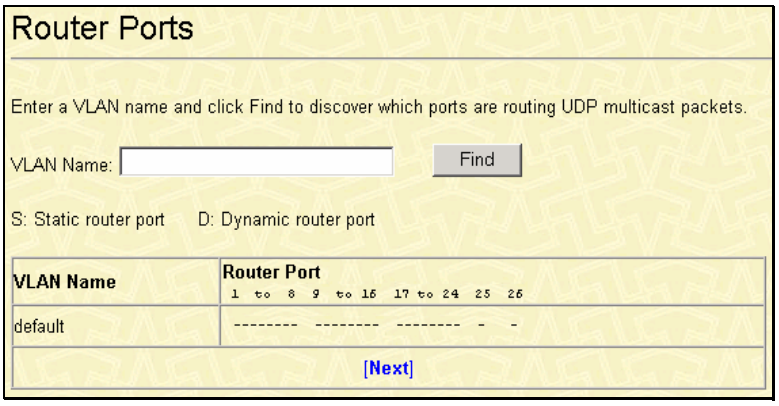


Figure 3-28: Router Ports window

IGMP Snooping Group Table

Click **Basic Setup > Network Monitoring > Status > IGMP Snooping Group Table**. This allows the switch's **IGMP Snooping Table** to be viewed. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch. The ports where the IGMP packets were snooped are displayed, signified with an M. The number of IGMP reports that were snooped is also displayed in the Reports field.

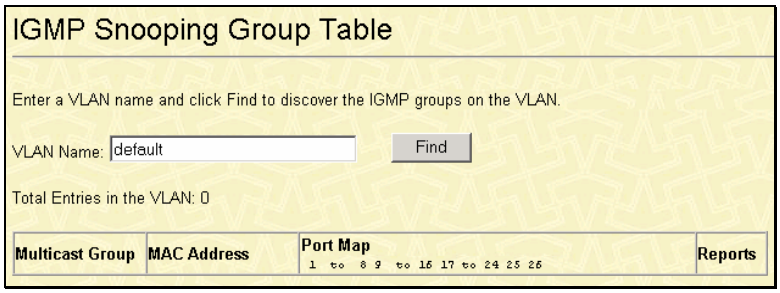


Figure 3-29: IGMP Snooping Group Table window

Switch History

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed.

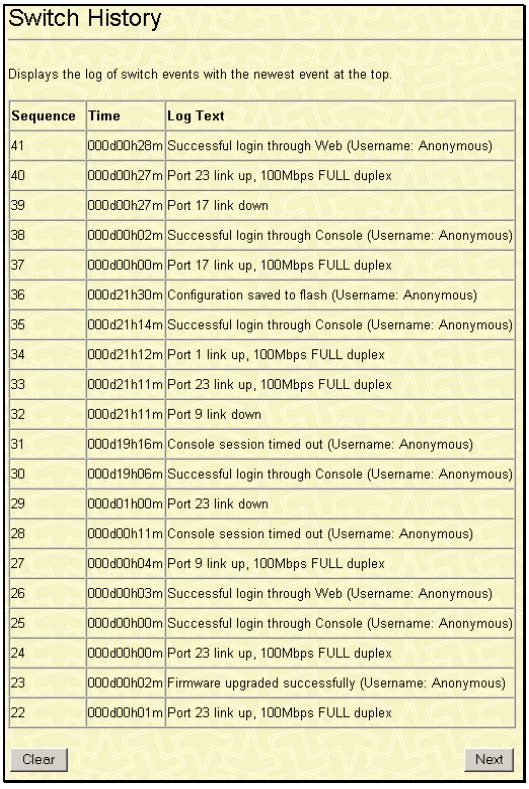


Figure 3-30: Switch History window

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Clicking **Next** at the bottom of the window will allow you to display all the switch Trap Logs.

The information is described as follows:

Parameter	Description
Sequence	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Displays the time in days, hours, and minutes since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

3.10. Factory Reset

The following window allows you to **Reset**, **Reset Config**, or **Reset System**. See the on-screen instructions for the differences among each option.

Note that all changes are kept in normal memory. If a user does not save the result into NV-RAM with the **Save Changes** function, the switch will recover all the settings the last user configured after the switch is rebooted.

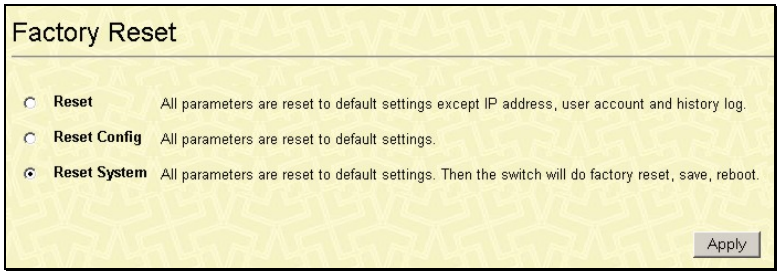


Figure 3-31: Factory Reset window

3.11. Save Changes

The LFSW-3226L has two levels of memory, normal RAM and non-volatile or NV-RAM.

To retain any configuration changes permanently, highlight **Save Changes** on the **Basic Setup** menu. The following windows will appear to verify that your new settings have been saved to NV-RAM.

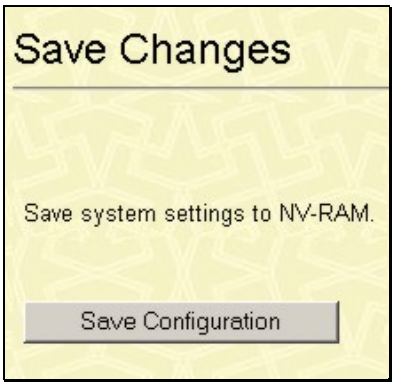


Figure 3-32: Save Changes window

3.12. Restart System

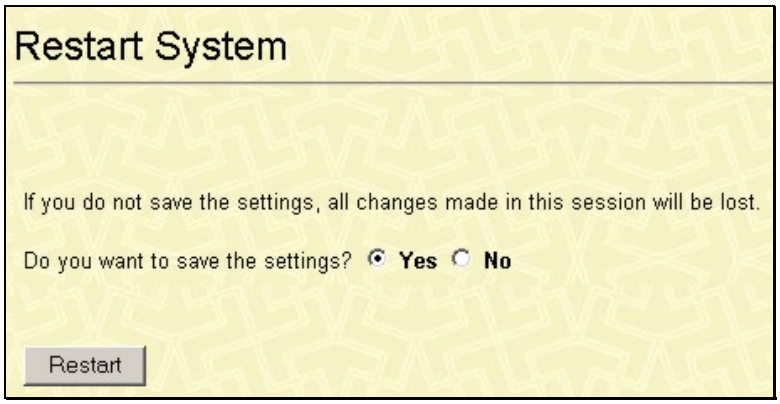


Figure 3-33: Restart System window

3.13. Logout

To logout off the switch, click the **Logout** link under the **Basic Setup** folder, which will present the following screen.

Figure 3-34: Web Logout Setup window.

To logout of the Web configuration, simply click Apply.

4. Switch Troubleshooting and Diagnostics

This chapter covers the following main topics:

- Failure types
- Troubleshooting Methods
- Technical support
- Return material authorization (RMA) procedures

The first step in troubleshooting is usually to go to the roof and confirm that the link heads are both receiving adequate power over the Free Space link. Many times the link heads will be blocked, misaligned, unplugged or have other simple problems. Go to the roof.

4.1. Failure Types

Three different kinds of failures can affect LFSW-3226L Switch performance:

- Failures caused by attached network components
- Failures caused by the environment
- LightPointe Switch failures

This troubleshooting section should be used in the event of a system failure. If a system failure occurs during initial installation, contact LightPointe Technical Support.

The most important error detection functions can be performed from the PC using the Management Port that allows you to pinpoint the failure precisely. More detailed troubleshooting can be done using FlightManager XA management interface window.

Caution: If a failure is found in the power supply unit, please remember that only authorized technical personnel may conduct checks of the power supply. In all cases, the system must be disconnected from the AC or DC power supply in advance of a service call.

4.1.1. Network Component Problems

There are a number of network-related problems that can cause the LFSW-3226L Switch to malfunction.

Table 4-1: Networking Equipment Problems

Network Problem	Effect on the LightPointe System
Bad network input signal	System failure, high BER, or low RSSI Link integrity LED is not illuminated on link head
Data input cable or connector damaged	No signal at the link head data input port or radio Link integrity LED is not illuminated on link head No failure between optical and RF High number of errors
Cable length violation	Low signal strength at the link head or radio The maximum length of a CAT-5 UTP cable in an Ethernet segment must not exceed 100 meters (328 feet)
Cables reversed (If applicable)	Management Port and Network cables are reversed. Incorrect signal at the link head
Free-space optical signal weak	Link failure
RF signal weak	Link failure
Wrong Switch port used	No communications, no fail over

4.2. Troubleshooting Methods

4.2.1. Ping Test to Check Configuration

You can use a laptop with Ethernet card to perform a ping test on the LightPointe XA Radios and Link heads. Factory default LightPointe system component IP addresses are found in Table 2-1.

Customer requested IP addresses are found in Table 2-2. The following equipment is required to perform a ping test.

- Laptop with Ethernet card
- Ethernet cable with RJ45 connectors

Step 1 Ensure the bench test system is interconnected correctly.

- Port #1 – Connected to a PC
- Port #24 – RF Unit (STP Enabled)
- **FlightLite 100/100E/155 and FlightStrata 155/100 XA**
  Port #22 – Linkhead Data (STP enabled)
  or
  FlightLite/FlightStrata G
  Port #25 for "G" Linkheads (STP enabled)

Step 2 Power up all equipment.

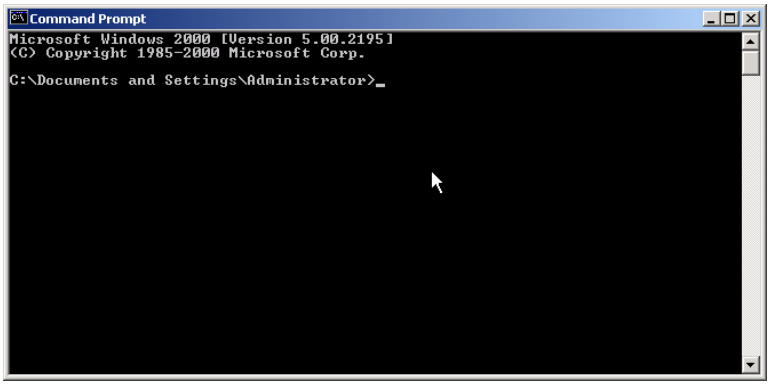
Step 3 Connect a PC to Port 26 of the Local or Peer Switch.

Step 4 Configure the PC IP Address and Subnet Mask.

- ❑ Use any IP address that wont conflict with current addresses (192.168.1.XXX)
- ❑ Use subnet mask 255 255 255 0

Step 5 Click the **Start** button on the PC and select the **Programs** option.

Step 6 ❑ Select the **MSDOS** prompt on the PC. The DOS window is displayed.



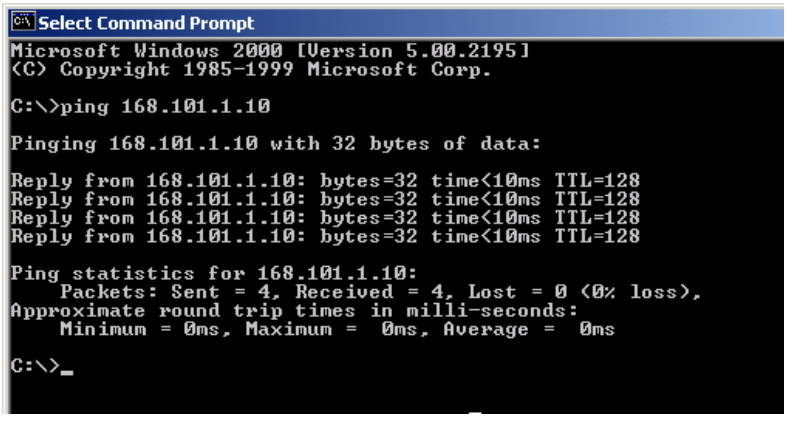
- ❑ Check the Switch only if you are unable to communicate with the link heads or RF units.

Step 7 To ping from the Local laptop, type in the Peer IP address: **ping 192.168.1.XXX.**

To ping from the Peer laptop, type in the Local IP address: **ping 192.168.1.XXX**.

To stop the ping tests, type **<Ctrl> C** on each laptop.

Step 8 A successful ping will display the following information on the PC screen.



Step 9 If you block the FOV (field of view) of the link head and ping, the PC screen should read "unreachable parameters".

Step 10 After completing ping tests, disconnect the PC cable from the Switch and replace the network cable.

4.2.2. FlightStrata 100 XA Switch Monitoring using a Web Browser

Step 1 Ensure the bench test system is interconnected correctly.

- ❑ Port #24 – RF Unit (STP Enabled)
- ❑ Port #22 – Linkhead Data (STP enabled)

Step 2 Connect an ethernet cable between port 1 and the ethernet port on a PC.

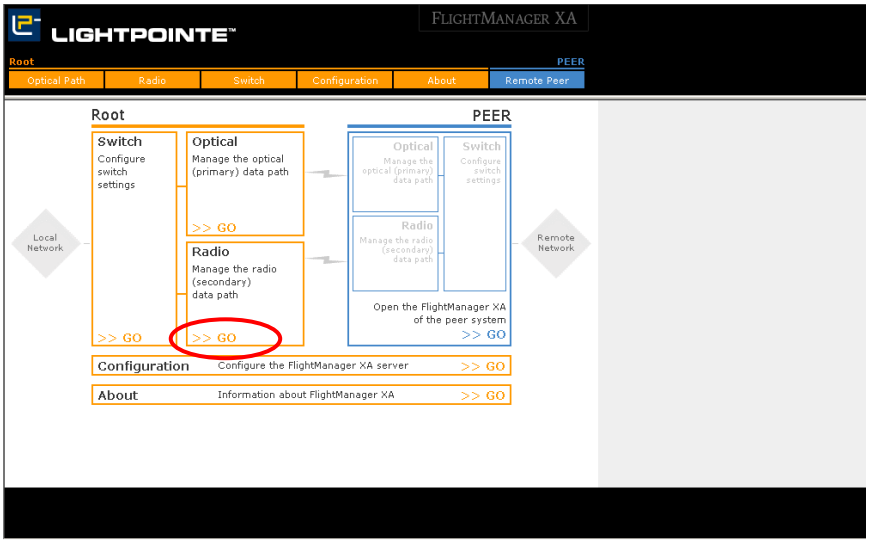
Step 3 ❑ Start up a Browser program on the PC.

❑ The system can be configured using a web browser such as Netscape® Navigator (version 6.2 and higher) or Microsoft® Internet Explorer (version 5.0 and higher)

Step 4 ❑ Enter the IP address of the desired link head (refer to Section 0). The Main FlightManager XA GUI window is displayed.

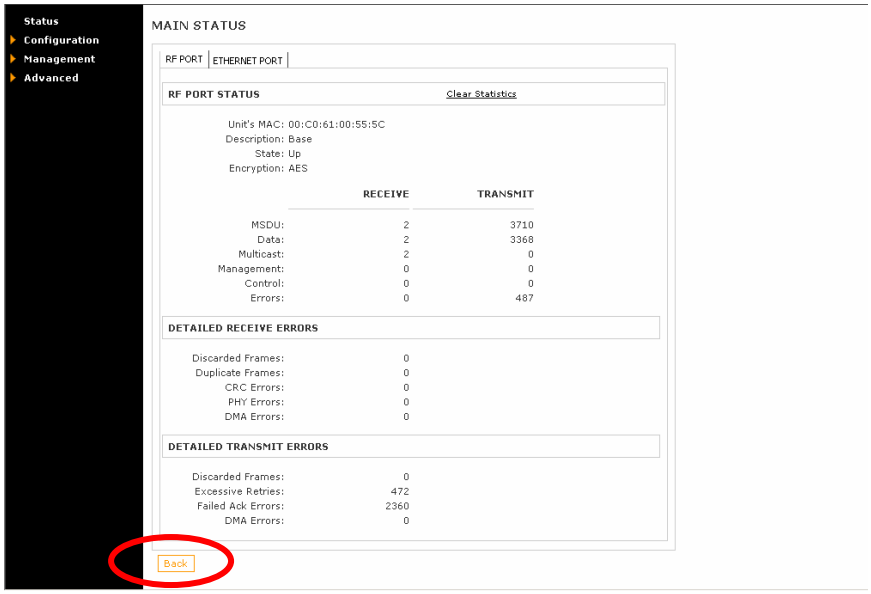
❑

Step 5 To open the Local Radio Web window from the Main FlightManager XA window, click on the Local Radio **GO** button. The Radio Main Status window is displayed.

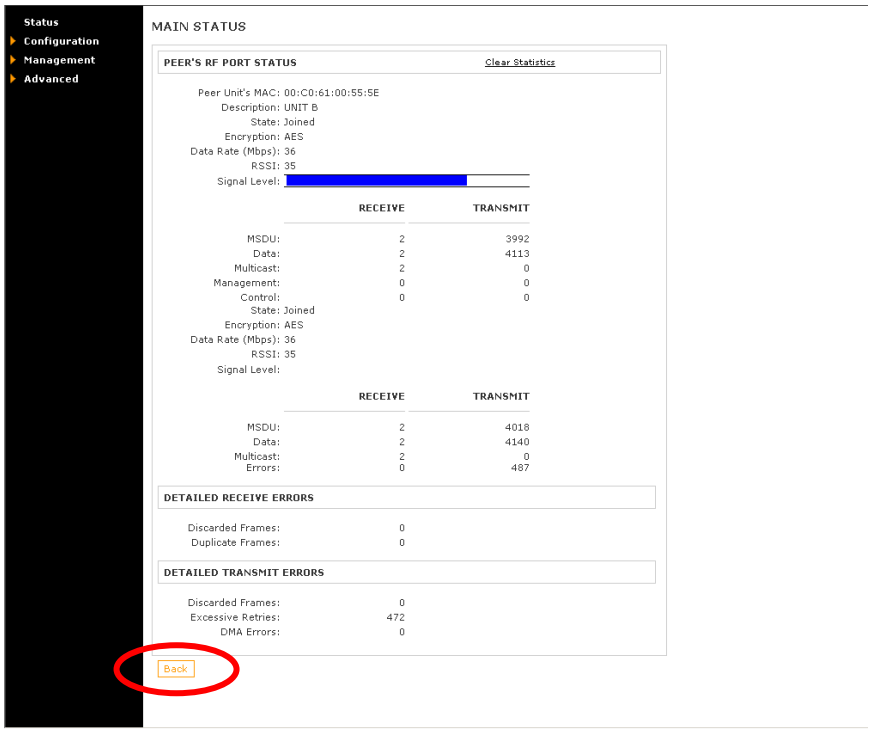


Step 6 To check the local radio receive and transmit data status, click on the upper MAC address. The Local Radio Status window is displayed.

❑ Click the Back button to return to the Main Status window.



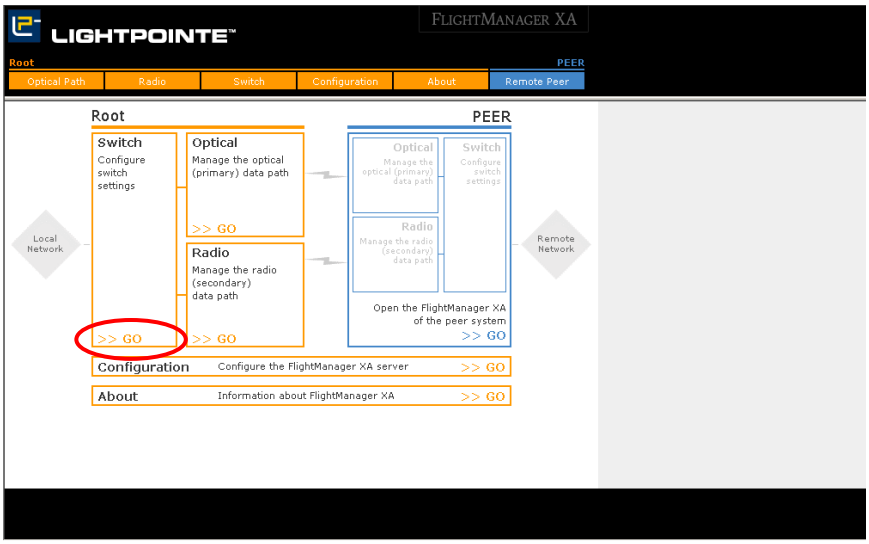
Step 7 To check the peer radio port and receive and transmit data status, click on the lower MAC address. The Peer Radio Status window is displayed.



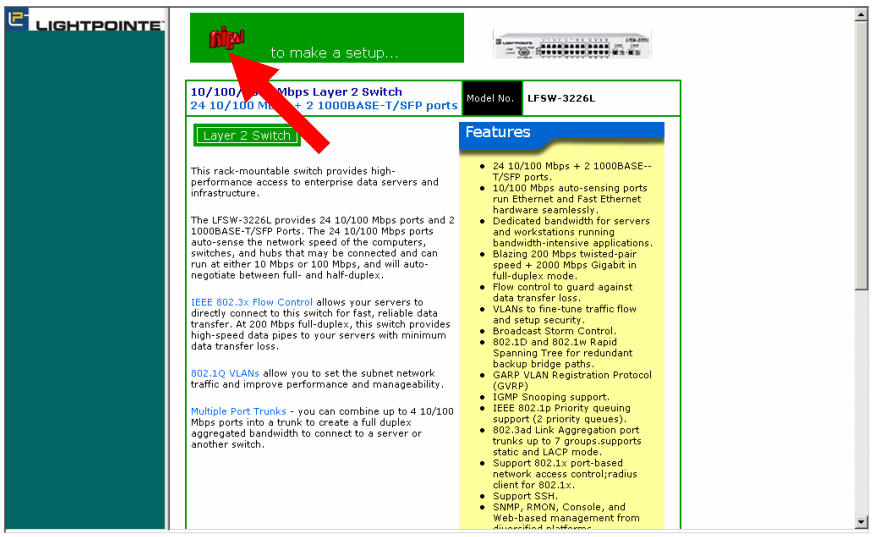
❑ Click the Back button to return to the Main Status window.

Step 8 To return to the FlightManager XA window, click on the LightPointe logo at the upper left corner of the window. The main FlightManager XA window is displayed.

Step 9 To verify local Switch operation, open the Switch Web window from the Main FlightManager XA window by clicking on the Switch **GO** button. The Switch Web window is displayed.



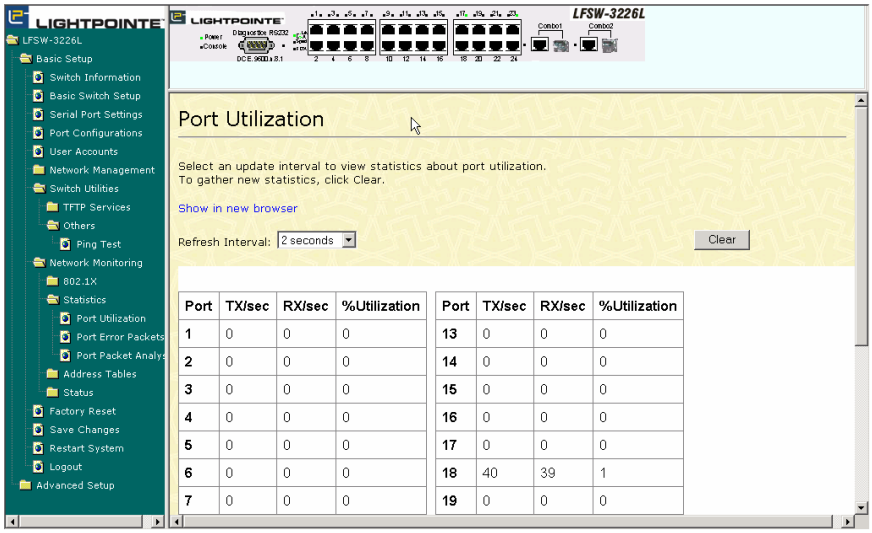
Step 10 To open the Logon window, click on the spinning logo. The Switch Information window is displayed.



Step 11 Click on **Basic Setup, Network Monitoring, Status,** and **Switch History** options. The Switch History window is displayed.

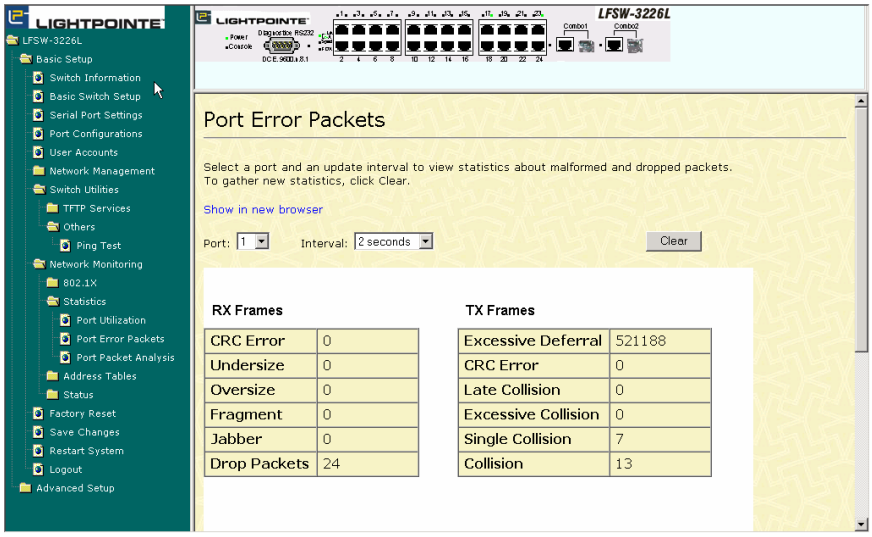
- ❑ View the Switch History window for any signs of errors.

Step 12 Click on **Basic Setup, Network Monitoring,** and **Statistics** options. The Port Utilization window is displayed.



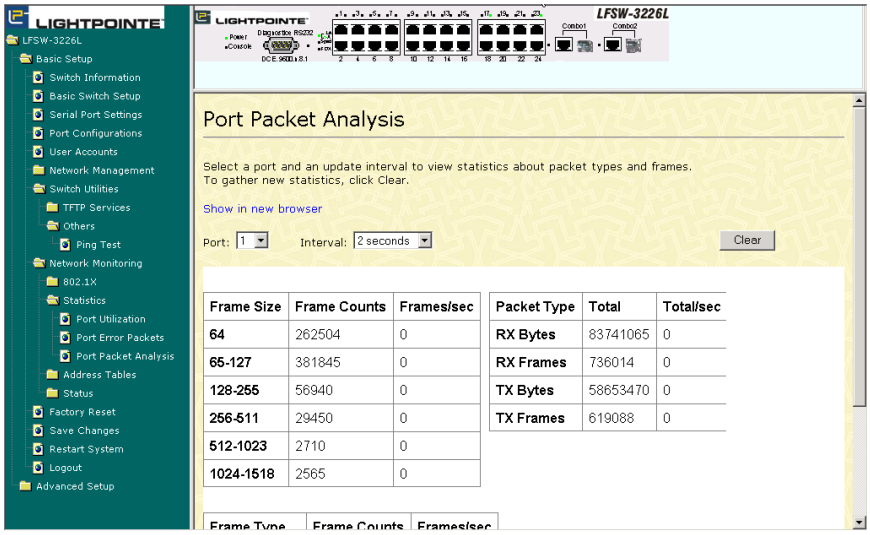
- ❑ View the Port Utilization window for any signs of errors.

Step 13 Click on **Port Error Packets** option. The Port Error Packets window is displayed.



- ❑ View the Port Error Packets window for any signs of errors.

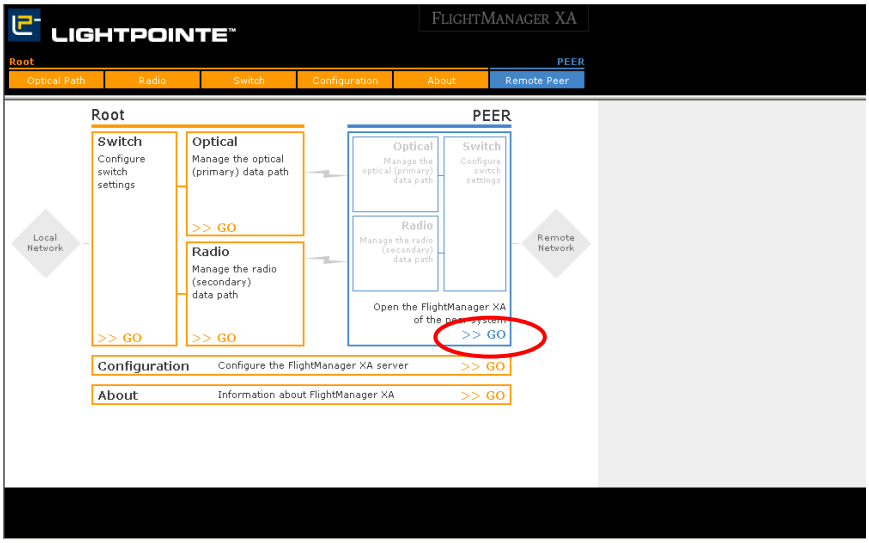
Step 14 Click on **Port Packet Analysis** option. The Port Error Packets window is displayed.



- ❑ View statistics about Port Packet Analysis window for any signs of errors.

Step 15 To return to the FlightManager XA window, click on the LightPointe logo at the upper left corner of the window. The main FlightManager XA window is displayed.

Step 16 To repeat the above steps on the Peer system, click on the Peer **GO** button. The Switch **GO** buttons on the left side of the window can now be used to access the Peer Switch.



Step 17 ❑ Exit the FlightManager XA program and disconnect the PC from the system. Reconnect the system (see Figure 2-2).

4.3. Technical Support

Did you complete the steps in the Fault Isolation Troubleshooting Tree?

4.3.1. Equipment Checklist Before You Call Technical Support

Be sure to fill out the following checklist before contacting LightPointe Technical Support.

General Information	Your Installation
❑ Application (Protocol)?	
❑ Distance?	
❑ How long has system been in operation?	
How does the error show up?	
❑ Temporary/permanent error?	
❑ Is error observed for the first time?	
How was the weather when error showed up?	
❑ What time of day?	
❑ Special weather conditions (fog, snowfall)	
❑ Outside temperature (moisture on entrance window)	
❑ Outside temperature (moisture on entrance window)	
Status of Back Panel LEDs	
❑ Are all red LEDs off?	Yes/No
❑ How many bars does the bar graph indicator show?	
Status of Back Panel Indicators	
❑ Connection to network	Yes/No
❑ Failure of endpoint equipment	Checked/Not Checked
What type of system is installed?	
❑ Model number	
❑ Serial number	
❑ Single mode or multimode (if applicable)	

Note: This form is available as a downloadable PDF file on our web site.

4.3.2. Return Material Authorization (RMA) Procedure

Please contact LightPointe before returning any system components for repair or replacement.

5. Specifications

Table 5-1: LFSW-3226L Switch Specifications

Product Information	Description	
General		
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z Gigabit Ethernet (over Fiber) IEEE 802.3ab Gigabit Ethernet IEEE 802.1Q Tagged VLAN IEEE 802.1P Tagged Packets IEEE 802.3ab 1000BASE-T IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 NWay auto-negotiation	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half duplex	Full duplex
Ethernet:	10 Mbps	20 Mbps
Fast Ethernet:	100 Mbps	200 Mbps
Gigabit Ethernet:	2000 Mbps (Full duplex only)	
Topology:	Star	
Network Cables		
10BASE-T:	UTP Category 3, 4, 5 (100 meters max.) EIA/TIA- 568 150-ohm STP (100 meters max.)	
100BASE-TX:	UTP Cat. 5 (100 meters max.) EIA/TIA-568 150-ohm STP (100 meters max.)	
1000BASE-T:	UTP Cat. 5e (100 meters max.) UTP Cat. 5 (100 meters max.) EIA/TIA-568B 150-ohm STP (100 meters max.)	
1000BASE-LX:	Single-mode fiber module (10km)	
1000BASE-SX	Multi-mode fiber module (550m)	
1000BASE-LHX:	Single-mode fiber module (40km)	
1000BASE-ZX:	Single-mode fiber module (80km)	
Mini-GBIC:	SFP Transceiver for 1000BASE-LX Single-mode fiber module (10km)	
Number of Ports:	24 10/100/1000 Mbps ports 2 1000BASE-T Mini-GBIC Combo Ports	
Performance		
Transmission Method:	Store-and-forward	
Packet Buffer:	3 MB per device	
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 1,488,095 pps per port (for 1000Mbps)	
MAC Address Learning:	Automatic update. Supports 4K MAC address.	

Product Information	Description
Priority Queues:	2 Priority Queues per port.
Forwarding Table Age Time:	Max age: 10–765 seconds. Default = 300.

Table 5-2: LFSW-3226L Switch Cable Lengths

Standard	Media Type	Maximum Distance
Mini-GBIC	1000BASE-LX, Single-mode fiber module	10km
	1000BASE-SX, Multi-mode fiber module	550m
	1000BASE-LHX, Single-mode fiber module	40km
	1000BASE-ZX, Single-mode fiber module	80km
1000BASE-T	Category 5e UTP Cable Category 5 UTP Cable (1000 Mbps)	100m
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m

Note: Use the above table to as a guide for the maximum cable lengths.

6. Index


LIGHTPOINTE™

A. Glossary

This Appendix contains a glossary of terms and acronyms used in this document.

1000BASE-LX: A long laser wavelength on multimode fiber optic cable for a maximum length of 10 kilometers.

1000BASE-SX: A short wavelength for a "long haul" fiber optic cable for a maximum length of 550 meters.

100BASE-FX: 100Mbps Ethernet implementation over fiber.

100BASE-TX: 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

10BASE-T: The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

ageing: The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM: Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

auto-negotiation: A feature on a port which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone port: A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

backbone: The part of a network used as the primary path for transporting traffic between network segments.

bandwidth: Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate: The switching speed of a line. Also known as line speed between network segments.

BOOTP: The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge: A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast: A message sent to all destination devices on the network.

broadcast storm: Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port: The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD: Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching: The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet: A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet: 100Mbps technology based on the Ethernet/CD network access method.

Flow Control: (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.

forwarding: The process of sending a packet toward its destination by an internetworking device.

full duplex: A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

GBIC: Gigabit Interface Connector

half duplex: A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

IP address: Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX: Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN: Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency: The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed: See baud rate.

main port: The port in a resilient link that carries data traffic in normal operating conditions.

MDI: Medium Dependent Interface. An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X: Medium Dependent Interface Cross-over. An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB: Management Information Base. Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast: Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol: A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link: A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.

RJ-45: Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON: Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS: Redundant Power System. A device that provides a backup source of power when connected to the Switch.

server farm: A cluster of servers in a centralized location serving a large user population.

SFP: Small Form Pluggable

SLIP: Serial Line Internet Protocol. A protocol which allows IP to run over a serial line connection.

SNMP: Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol (STP): A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

stack: A group of network devices that are integrated to form a single logical device.

standby port: The port in a resilient link that will take over data transmission if the main port in the link fails.

switch: A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP: A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

telnet: A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP: Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.

UDP: User Datagram Protocol. An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN: Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT: Virtual LAN Trunk. A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100: A type of terminal which uses ASCII characters. VT100 screens have a text-based appearance.

B. Advanced Switch Settings

This appendix contains a detailed discussion about some of the advanced functions of the switch, including:

- Port Segmentation
- Spanning Tree
- Forwarding
- Configure QoS
- Mirroring Configurations
- VLAN Configurations
- Link Aggregation
- 802.1x
- System Log
- Multicast Configurations
- SSH Management.

NOTE: The LFSW-3226L switch has been customized and pre-configured to ensure optimal performance in LightPointe optical wireless installations. Any changes to default settings or use of advanced switch features may impact the operation of the optical wireless link.

B.1. Port Segmentation

The Port Segmentation window contains **Load Port Segmentation**.

B.1.1. Load Port Segmentation

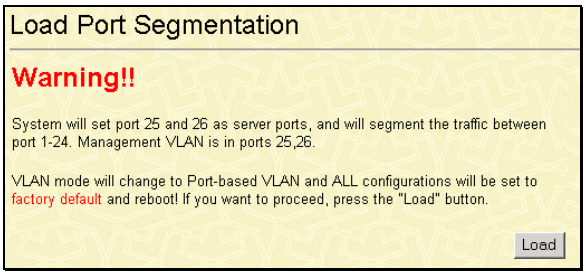


Figure B-1: Load Port Segmentation window

B.2. Spanning Tree

The switch supports 802.1d Spanning Tree Protocol (STP). 802.1d STP will be familiar to most networking professionals and may be configured on this switch as follows:

B.2.1. STP Switch Settings

To globally configure STP on the Switch, under **Advanced Setup**, click **Spanning Tree** and then **STP Switch Settings**.

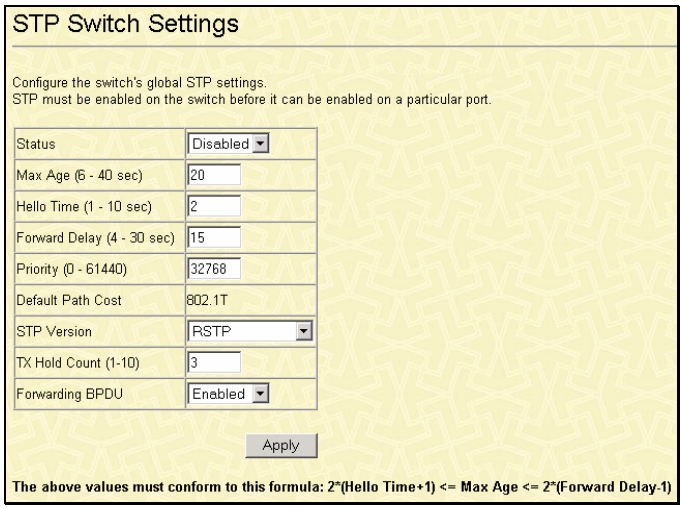


Figure B-2: STP Switch Settings window

The Switch supports 801.2d Spanning Tree Protocol, which allows you to create alternative paths (with multiple switches or other types of bridges) in your network.

Click **Apply** after making changes to the window above.

Parameters that you can change are:

Parameter	Description
Status	This drop-down menu allows you to enable the Spanning Tree Protocol setting.
Max. Age (6-40 sec)	<20> – The Maximum Age can be from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root Bridge, your switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge.
Hello Time (1-10 sec)	<2> – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a Hello Time for your switch, and it is not the Root Bridge, the set Hello Time will be used if and when your switch becomes the Root Bridge.
Forward Delay (4-30 sec)	<15> – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.
Priority (0-61440)	<32768> – A Bridge Priority can be from 0 to 61,440. Zero is equal to the highest Bridge Priority.
STP Version	Choose RSTP or STP compatible. Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment.
TX Hold Count (1-10)	This is the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default value is 3
Forwarding BPDU	This can be Enabled or Disabled. When it is enabled it allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled.

Note: Observe the following formulas when setting the above parameters:
Max. Age ≤ 2 x (Forward Delay - 1 second)
Max. Age ≥ 2 x (Hello Time + 1 second)

Note: The Spanning Tree Protocol (STP) operates on two levels: On the switch level, the settings are globally implemented. On the port level, the settings are implemented on a per user-defined Group basis.

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

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

B.2.2. STP Port Settings

To configure STP Port Settings on the Switch, under Advanced Setup, click Spanning Tree and then STP Port Settings.

STP Port Table

Edit

	Port	Connection	State	Cost	Pri	Edge	P2P	Status	Role
○	1	100M/Full/None	Yes	*200000	128	No	Yes	Forwarding	NonStp
○	2	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	3	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	4	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	5	100M/Full/None	Yes	*200000	128	No	Yes	Forwarding	NonStp
○	6	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	7	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	8	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	9	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	10	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	11	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	12	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	13	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	14	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	15	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	16	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	17	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	18	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	19	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	20	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	21	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	22	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	23	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	24	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	25	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
○	26	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled

Figure B-3: STP Port Table window

Select an entry on the STP Port Table and then click **Edit**:

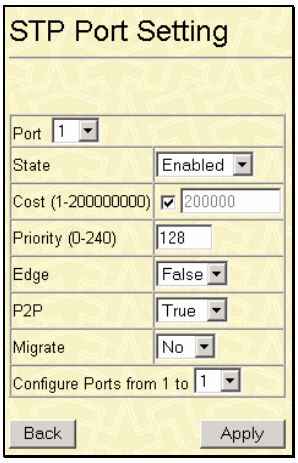


Figure B-4: STP Port Setting window

The STP port settings that can be configured are:

Parameter	Description
Port	Number of port being configured.
State	Toggle between Enabled and Disabled. When STP is enabled, a change from link-down to link-up will trigger the Spanning Tree Protocol. STP will set the port to the listening state. After the forward delay, STP will set the port to the learning state. After another forward delay, STP will set the port to the forwarding state. If the forward delay is 15 seconds, the port will take 30 seconds to forward packets. However, when Fast STP is Enabled on a port, the port will only take 15 seconds from link-up to the time it starts forwarding packets. This is because enabling the Fast STP option will skip the learning state, jumping directly to the forwarding state from the listening state.
Cost (1-200000000)	A Port Cost can be set from 1 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.
Priority (0-240)	A Port Priority can be from 0 to 255. The lower the number, the greater the probability the port will be chosen as the Root Port.
Edge	Select True or False. Choosing True designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. False indicates the port does not have edge port status.
P2P	Select True, False, or Auto. Choosing True indicates a point-to-point (p2p) shared link. These are similar to edge ports however they are restricted in that a p2p port must operate in full duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP. The Auto setting instructs the switch to force a connection to a non-P2P port when it detects 1 or more BPDUs.
Migrate	Select Yes or No. Choosing Yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (Yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment
Configure Ports from 1 to	A consecutive group of ports may be configured starting with the selected port.

To configure **Spanning Tree Protocol** functions for individual ports, enter the desired information in the fields on this window (see the descriptions below for assistance) and then click **Apply**.

B.3. Forwarding

The Switch supports MAC forwarding.

B.3.1. MAC Forwarding

The MAC Forwarding feature is divided between MAC Address Aging Time and Configure The Broadcast Storm Control Mode.

MAC Address Aging Time

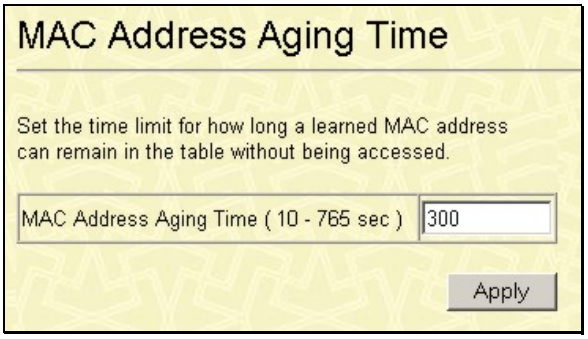


Figure B-5: MAC Address Aging Time window

The **MAC Address Aging Time** field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between 10 and 765 seconds.

Note: A very long Aging Time can result with the out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions. A very short aging time may cause entries to be aged out too soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Configure The Broadcast Storm Control Mode

This field can be toggled between Enable and Disable using the drop-down menu. This enables or disables, globally, the Switch's reaction to Broadcast storms, triggered at the threshold set in the last field.

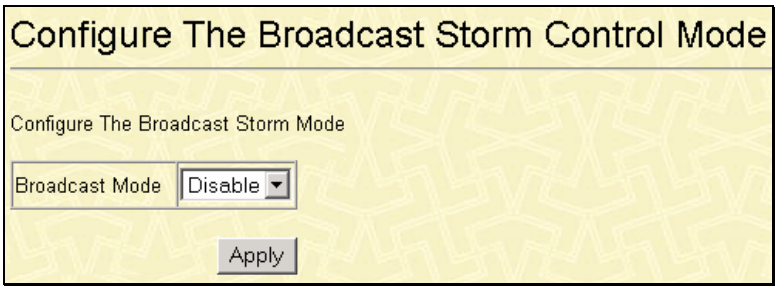


Figure B-6: Configure The Broadcast Storm Control Mode window

B.4. Configure QoS

The LFSW-3226L supports 802.1p priority queuing. The switch has two priority queues. These priority queues are labeled as 0, the high queue, and 1, the low queue. These priority queues, specified in IEEE 802.1p are mapped to the switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q0 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q0 queue.
- Priority 3 is assigned to the Switch's Q0 queue.
- Priority 4 is assigned to the Switch's Q1 queue.
- Priority 5 is assigned to the Switch's Q1 queue.
- Priority 6 is assigned to the Switch's Q1 queue.
- Priority 7 is assigned to the Switch's Q1 queue.

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

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of eight CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the LFSW-3226L has two priority queues (and thus two Classes of Service) for each port on the switch.

B.4.1. 802.1p User Priority

The LFSW-3226L allows the assignment of a User Priority to each of the 802.1p priorities.

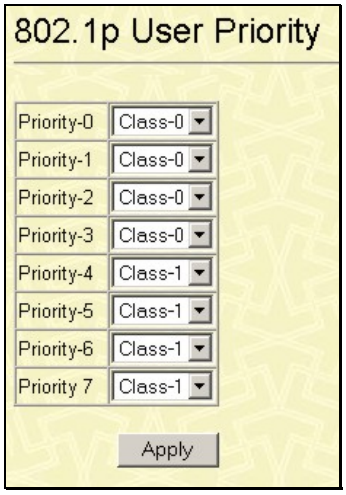


Figure B-7: 802.1p User Priority window

Once you have assigned a priority to the port groups on the switch, you can then assign this Class to each of the eight levels of 802.1p priorities.

Note: The settings you assign to the queues, numbers 0-1, represent the IEEE 802.1p priority tag number. Do not confuse these settings with port numbers.

B.4.2. QoS Scheduling Mechanism

This drop-down menu allows you to select between a **Weight Fair** and a **Strict** mechanism for emptying the priority classes. In the **Configuration** menu open the **QoS** folder and click **QoS Scheduling Mechanism**, to view the screen shown below.

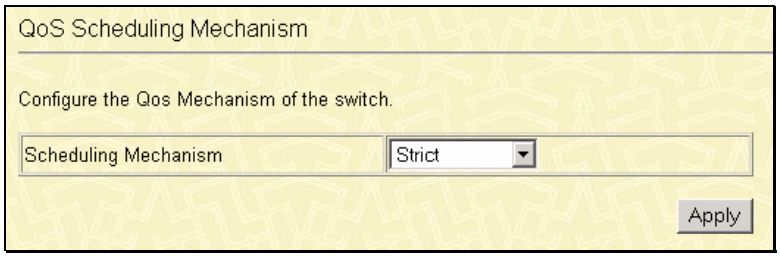


Figure B-8: The Scheduling Mechanism has the following parameters:

Parameter	Description
Strict	The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.
Round Robin	Use the round robin algorithm to handle packets in an even distribution in priority classes of service.

B.4.3. Bandwidth Control Table

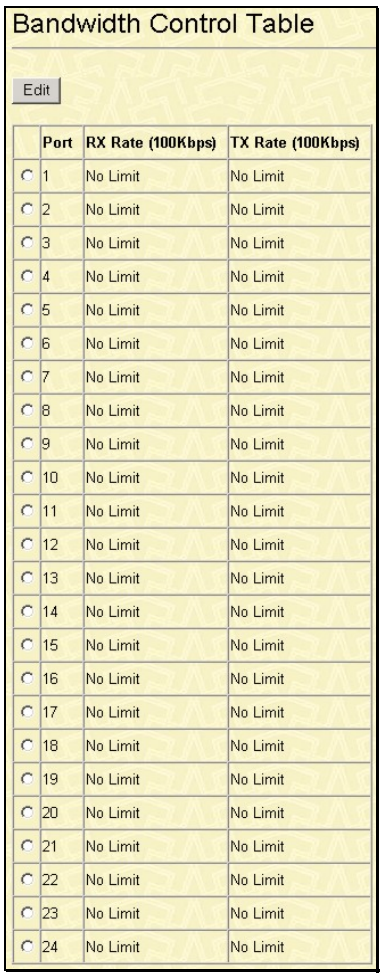


Figure B-9: Bandwidth Control Table window

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data bit rates for any port.

To change the maximum allowed bandwidth for a given port in the **Bandwidth Control Table** window, click the selection button in the far left column that corresponds to the port you want to configure and click the **Edit** button. A new window opens:

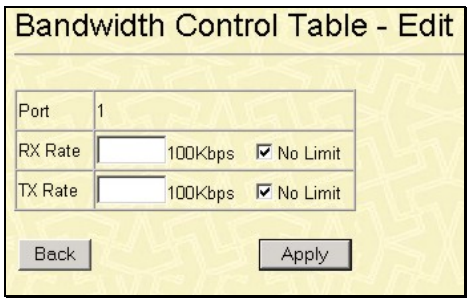


Figure B-10: Bandwidth Control Table – Edit window

To limit either the RX or TX rates, deselect the No Limit check box and enter the desired rate. Rates can be expressed using whole numbers up to the maximum available rate for the port.

B.5. Mirroring Configurations

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes. To view the **Mirror Configurations** window, click **Advanced Setup > Mirroring Configurations**.

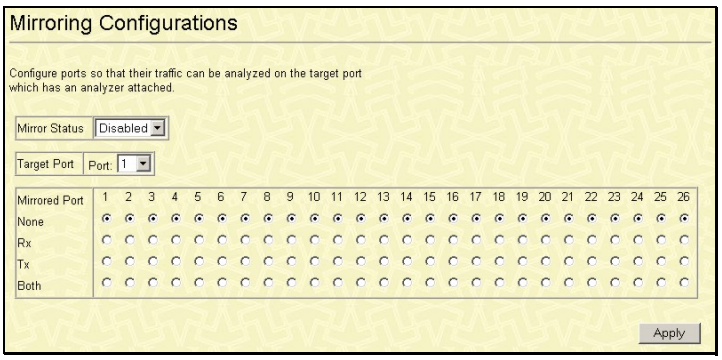


Figure B-11: Mirroring Configurations window

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

Up to 25 entries can be made to the port mirroring table, but it should be noted that a faster port (a 1000 Mbps Gigabit Ethernet port, for example) should not be mirrored to a slower port, because many packets will be dropped.

The following fields can be set:

Field	Description
Mirror Status	This enables or disables mirroring.
Target Port	This is the port where information will be duplicated and sent for capture and network analysis.
Mirrored Port	This field can be toggled among None, Both, Rx and Tx. Rx mirrors only received packets, while Tx mirrors only transmitted packets.

Note: You should not mirror a faster port or higher traffic ports on a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies.

B.6. VLAN Configurations

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 1, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

A weighted round robin system is employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 1, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLANs

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

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

Notes about VLANs on the LFSW-3226L:

- No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets **cannot** cross VLANs without a network device performing a routing function between the VLANs.
- The LFSW-3226L supports IEEE 802.1Q VLANs and Port-Based VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
- The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
- The "default" has a VID = 1.
- The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

Tagging – The act of putting 802.1Q VLAN information into the header of a packet.

Untagging – The act of stripping 802.1Q VLAN information out of the packet header.

Ingress port – A port on a switch where packets are flowing into the switch and VLAN decisions must be made.

Egress port – A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

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

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

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

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.

802.1Q VLAN Packet Forwarding

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

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

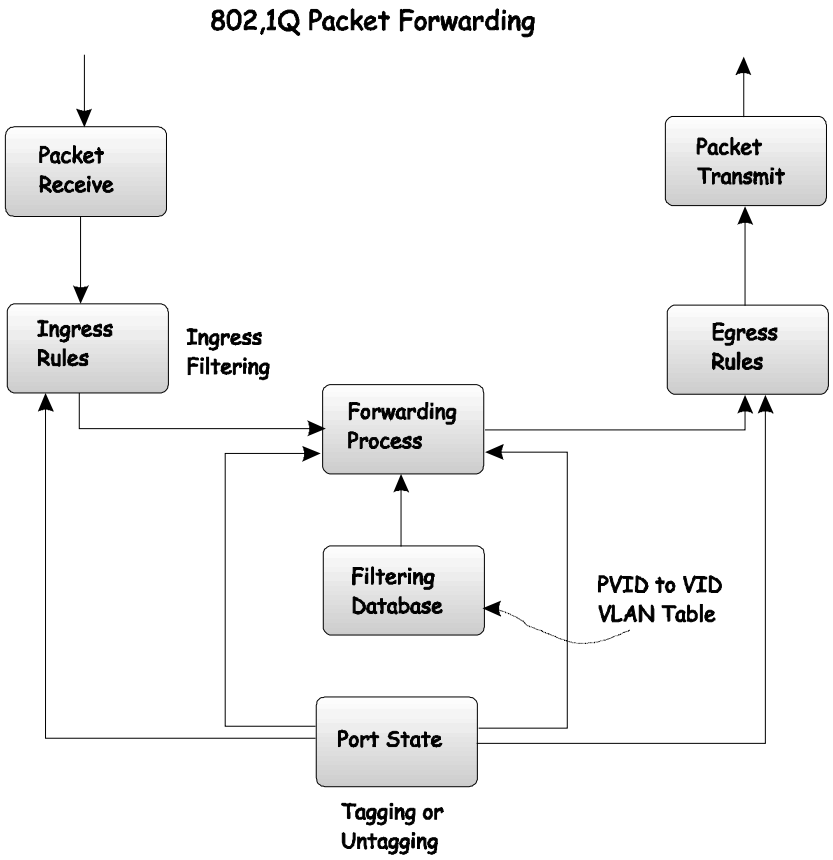


Figure B-12: IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

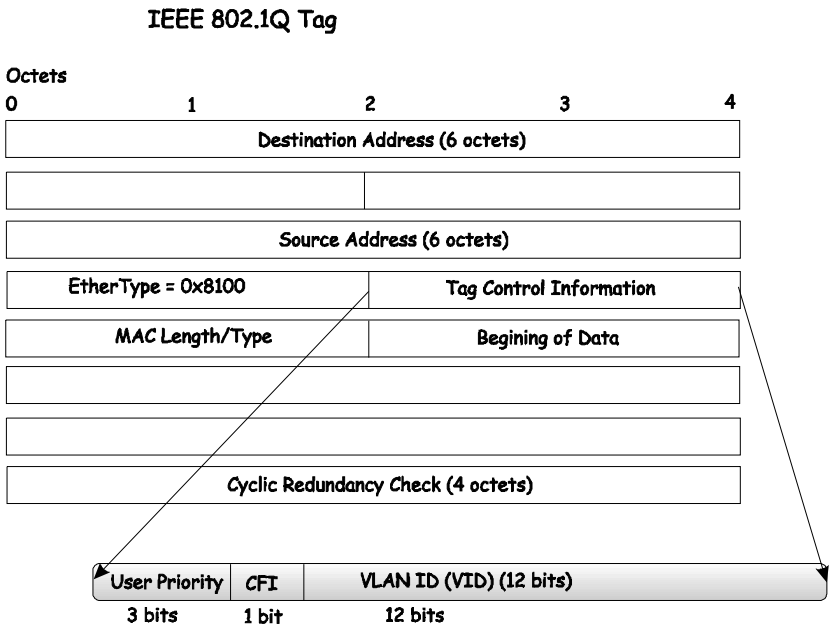


Figure B-13: IEEE 802.1Q Tag

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

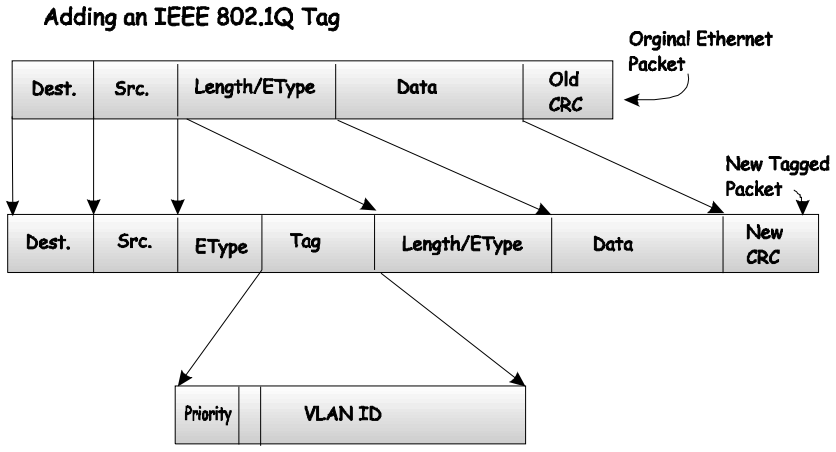


Figure B-14: Adding an IEEE 802.1Q Tag

Port VLAN ID

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

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

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the switch will drop the packet.

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

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

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

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

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

Tagging and Untagging

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

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

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

Ingress Filtering

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

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

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

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

Initial VLAN Configuration

The Switch initially configures one VLAN, VID = 1, called the "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

Note: If no VLANs are configured on the switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	AssignedS Ports
System (default)	5, 6, 7, 8, 21, 22, 23, 24
Engineering	9, 10, 11, 12
Marketing	13, 14, 15, 16
Finance	17, 18, 19, 20
Sales	1, 2, 3, 4

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

Network resources such as printers and servers however, can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, setting VLAN 1 members to ports 1, 2, 3, and 4 and VLAN 2 members to ports 1, 5, 6, and 7. Port 1 belongs to two VLAN groups. Ports 8, 9, and 10 are not configured to any VLAN group. This means ports 8, 9, and 10 are in the same VLAN group.

VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

Note: In order to use VLAN segmentation in conjunction with port trunk groups, you can first set the port trunk group(s), and then you may configure VLAN settings. If you wish to change the port trunk grouping with VLANs already in place, you will not need to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

B.6.1. VLAN Mode Set

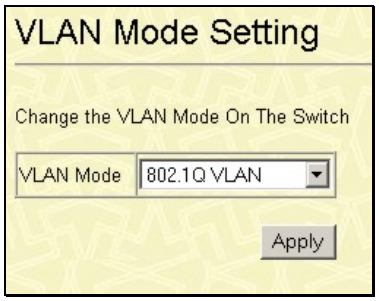


Figure B-15: VLAN Mode Setting window

This screen is used to change the VLAN Setting on the Switch. The user may use the pull-down menu to choose between **802.1Q VLAN** and **Port-Based VLAN.** After choosing a different VLAN mode, click **Apply** and the Switch will have to reboot to apply the settings.

B.6.2. Switch GVRP

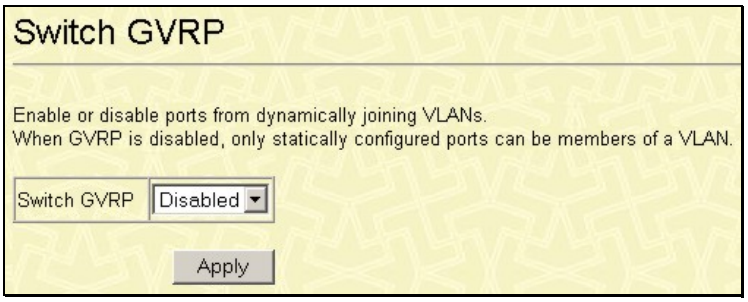


Figure B-16: Switch GVRP window

The **Group VLAN Registration Protocol (GVRP**) enables the port to dynamically become a member of a VLAN. **GVRP** is Disabled by default.

B.6.3. 802.1Q VLANs

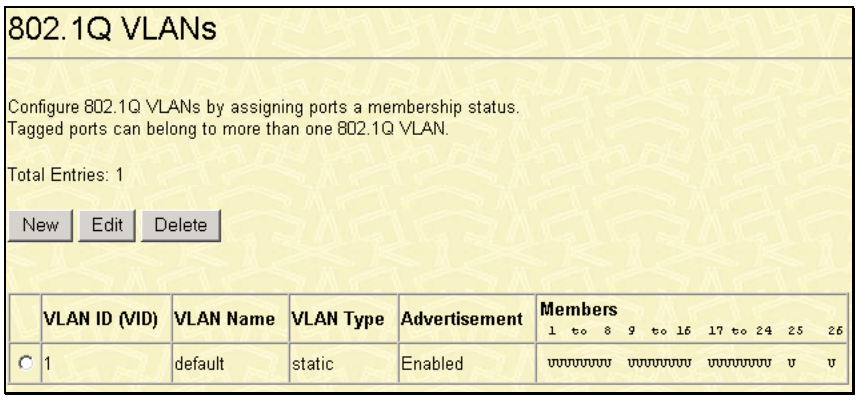


Figure B-17: 802.1Q VLANs window

To delete an existing 802.1Q VLAN, click the corresponding radio button to the left of the VLAN you want to delete from the Switch and then click the **Delete** button.

Parameter	Description
VLAN ID (VID)	The VLAN ID of the VLAN that was created.
VLAN Name	The name of the VLAN that is being created.
VLAN Type	This indicates the type of VLAN, static or LACP.
Advertisement	Enabling this function will allow the switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Members	Corresponds to the ports that are members of the particular VLAN.

To create a new **802.1Q VLAN**, click the **New** button:

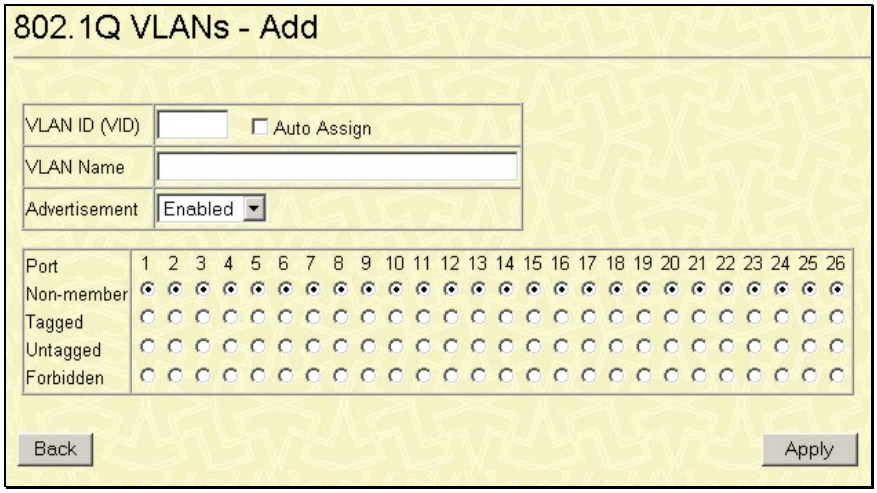


Figure B-18: 802.1Q VLANs – Add window

To edit an existing VLAN, click **Edit**, which will reveal the following screen.

Note: The Switch's default is to assign all ports to a single VLAN named "default". As new VLANs are created, the member ports assigned to the new VLAN will be removed from the default VLAN port member list. (This is specific to port-based VLANs only).

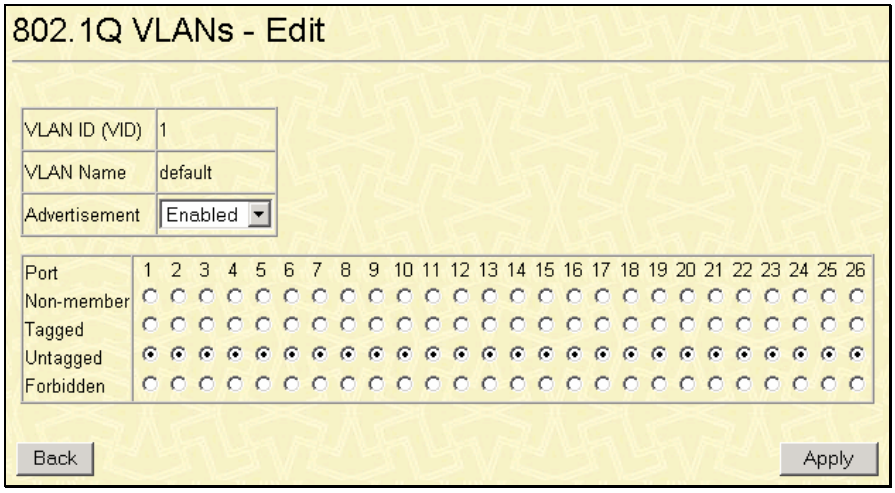


Figure B-19: 802.1Q VLANs – Edit window

Both of these windows offer the following fields to configure:

Parameter	Description
VLAN ID (VID)	Allows the entry of a VLAN ID in the Add window, or displays the VLAN ID of an existing VLAN in the Modify window. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN in the Add window.
Advertisement	Advertising can be enabled or disabled using this pull-down menu. By disabling the Advertisement function, the Switch does not send any GARP/GVRP messages of the VLAN.
Port	Allows an individual port to be specified as member of a VLAN.
Non-member	Allows an individual port to be specified as a non-VLAN member.
Tagged/Untagged	Allows an individual port to be specified as Tagged or Untagged. A check in the Tagged field specifies the port as a Tagging member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the VID (VLAN Identifier – see below). When a tagged packet exits the port, the packet header is unchanged. A check in the Untagged field specifies the port as an Un-tagging member of the VLAN. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.
Forbidden	Forbidden Non-Member - specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

B.6.4. IEEE 802.1Q Port Settings

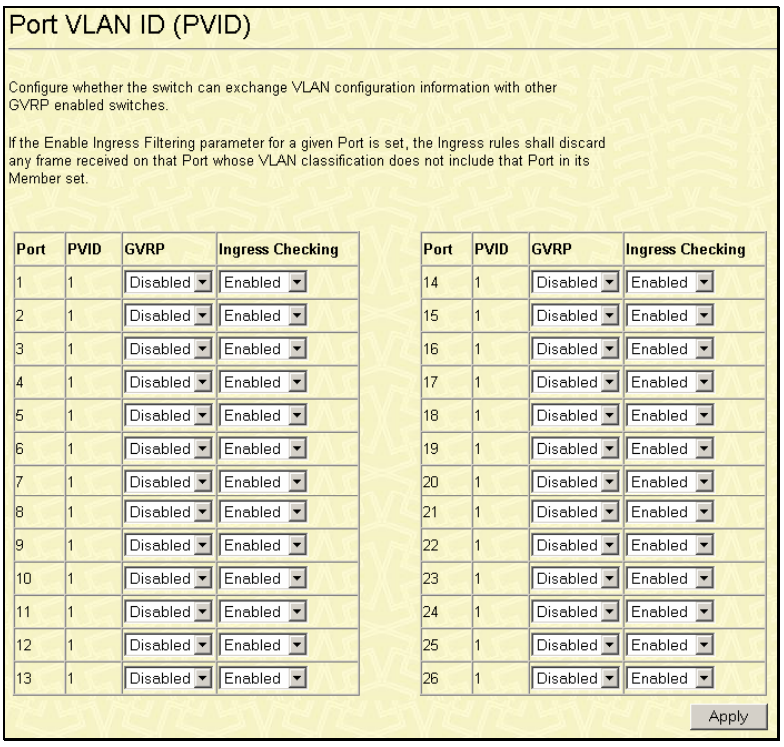


Figure B-20: Port VLAN ID (PVID) window

This window allows you to see a **Port VLAN ID (PVID)** number, enable or disable the ingress filtering check, and enable or disable GVRP for individual ports.

Ingress filtering means that a receiving port will check to see if it is a member of the VLAN ID in the packet before forwarding the packet. GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q ports. With GVRP, the Switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q ports. Click **Apply** to allow your changes to take effect.

The information on the window is described as follows:

Parameter	Description
Port	Corresponding number to a port on the switch.
PVID	PVID is used to decide whether received untagged packets belong to a VLAN.
GVRP	For each corresponding port, GARP VLAN Registration Protocol can be Enabled or Disabled.
Ingress Checking	Ingress checking is used to check if the received port is a member port of the VLAN whose VID is equal to the VID of incoming packets. If not, the ingress checking will drop the packets.

B.7. Link Aggregation

B.7.1. Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.

The LFSW-3226L supports up to seven port trunk groups with two to four ports in each group. A potential bit rate of 800 Mbps can be achieved.

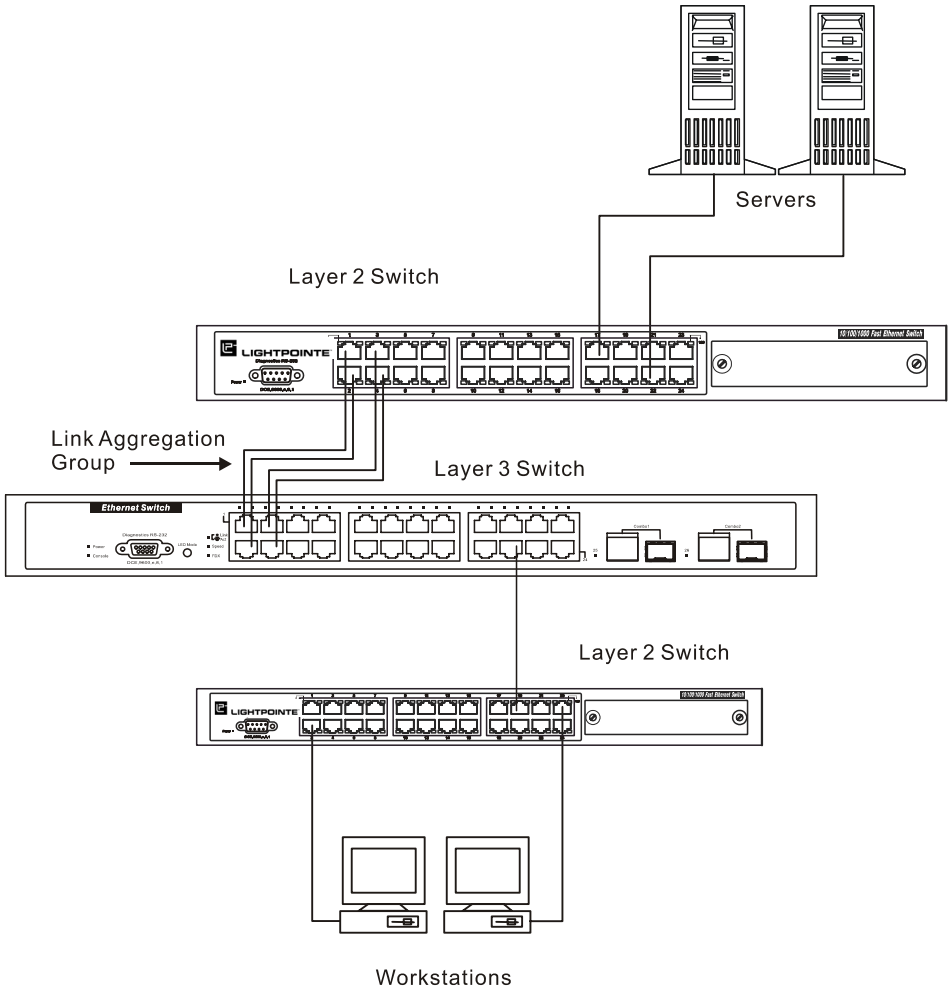


Figure B-21: Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent. A trunk connection can be made with any other switch that maintains host-to-host data streams over a single trunk port. Switches that use a load-balancing scheme and send packets of a host-to-host data stream over multiple trunk ports cannot have a trunk connection with the Switch.

Note: If the two external module ports are used as a trunk group and either port is disconnected, packets intended for the disconnected port will be dropped.

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

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

The switch allows the creation of up to seven link aggregation groups, each group consisting of up of up to four links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the two (optional) Gigabit ports, which can only belong to a single link aggregation group. A link aggregation group may not cross an 8-port boundary, starting with port 1 (a group may not contain ports 8 and 9, for example) and all of the ports in the group must be members of the same VLAN. Further, the aggregated links must all be of the same speed and should be configured as full duplex.

The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the aggregation group. This port is called the Master Port of the group, and all configuration options, including the VLAN configuration, that can be applied to the Master Port are applied to the entire link aggregation group.

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

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

B.7.2. Link Aggregation Group

To configure port trunking, click on **Link Aggregation** and then **Link Aggregation Group** in the **Advanced Setup** folder to bring up the **Link Aggregation** table:

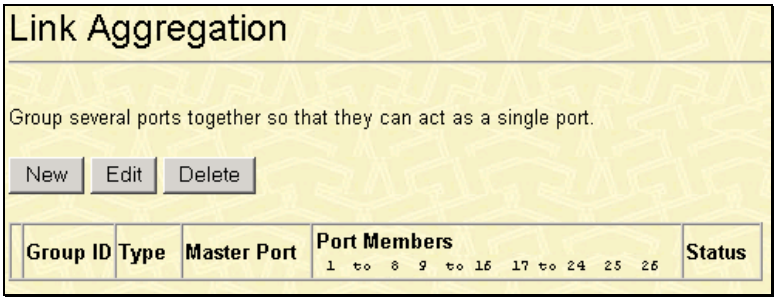


Figure B-22: 1st Link Aggregation window

Click **New** to create a new link aggregation:

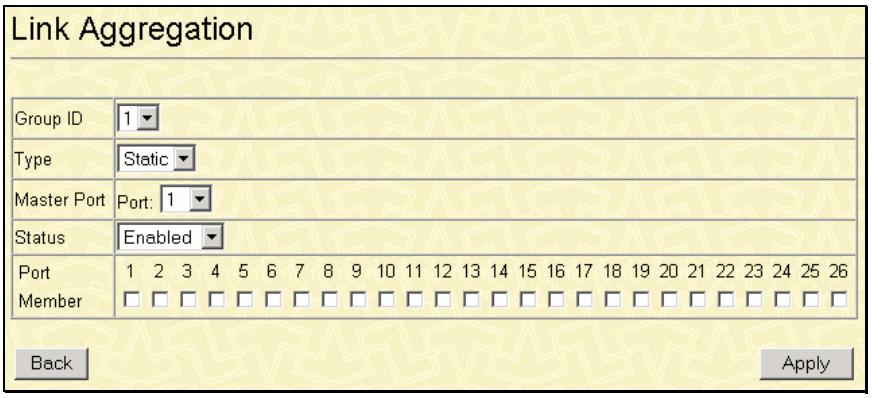


Figure B-23: 2nd Link Aggregation window

The following fields can be set:

Parameter	Description
Group ID	Allows the entry of a number used to identify the link aggregation group, when adding a new group. Displays the Group ID of the currently selected link aggregation group, when editing and existing entry.
Type	Toggle to determine which type of link aggregation to use, Static or LACP.
Master Port	The Master port of link aggregation group.
Status	This field can be toggled between Enabled and Disabled. This is used to turn a link aggregation group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup link aggregation group that is not under automatic control.

B.7.3. LACP Port Config

LACP supports the automatic creation of link aggregation by exchanging LACP packets between LAN ports. LACP packets are exchanged only between ports in passive and active modes. Both the passive and active modes allow LACP to negotiate between LAN ports to determine if they can form a link aggregation.

Passive – LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. This is the default.

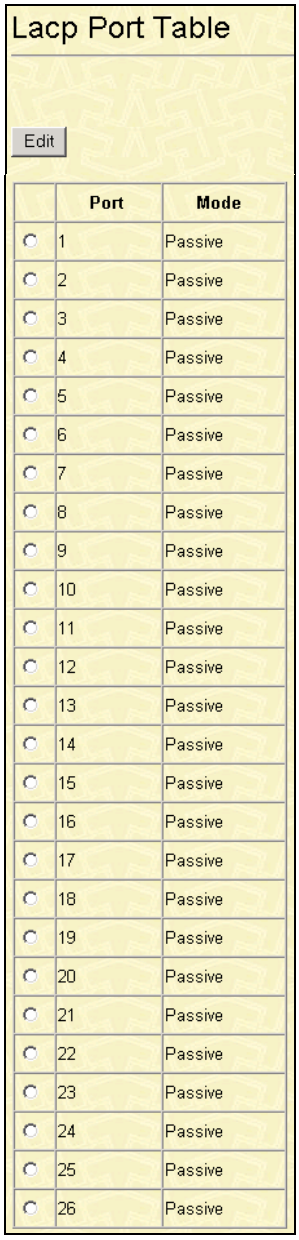
Active – LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.

LAN ports can form a trunk group when they are in different LACP modes as long as the modes are compatible. For example:

A LAN port in active mode can form a trunk group successfully with another LAN port that is in active mode.

A LAN port in active mode can form a trunk group with another LAN port in passive mode.

A LAN port in passive mode cannot form a trunk with another LAN port that is also in passive mode, because neither port will initiate negotiation.



	Port	Mode
○	1	Passive
○	2	Passive
○	3	Passive
○	4	Passive
○	5	Passive
○	6	Passive
○	7	Passive
○	8	Passive
○	9	Passive
○	10	Passive
○	11	Passive
○	12	Passive
○	13	Passive
○	14	Passive
○	15	Passive
○	16	Passive
○	17	Passive
○	18	Passive
○	19	Passive
○	20	Passive
○	21	Passive
○	22	Passive
○	23	Passive
○	24	Passive
○	25	Passive
○	26	Passive

Figure B-24: LACP Port Table window

To edit an LACP Port Table entry, select it and then click **Edit**.

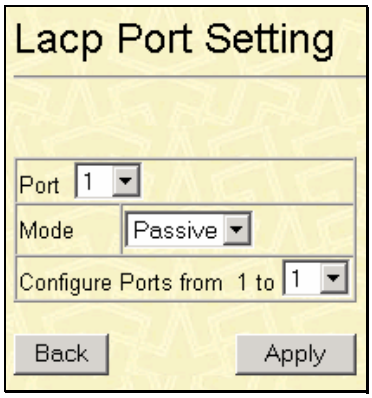


Figure B-25: LACP Port Setting window

Select the desired port, mode, and range of ports to be configured and then click **Apply**.

B.8. 802.1x

The Switch is an implementation of the server side of IEEE 802.1x Port-Based Network Access Control. Through this mechanism, users have to be authorized before being able to access the network. See the following figure:

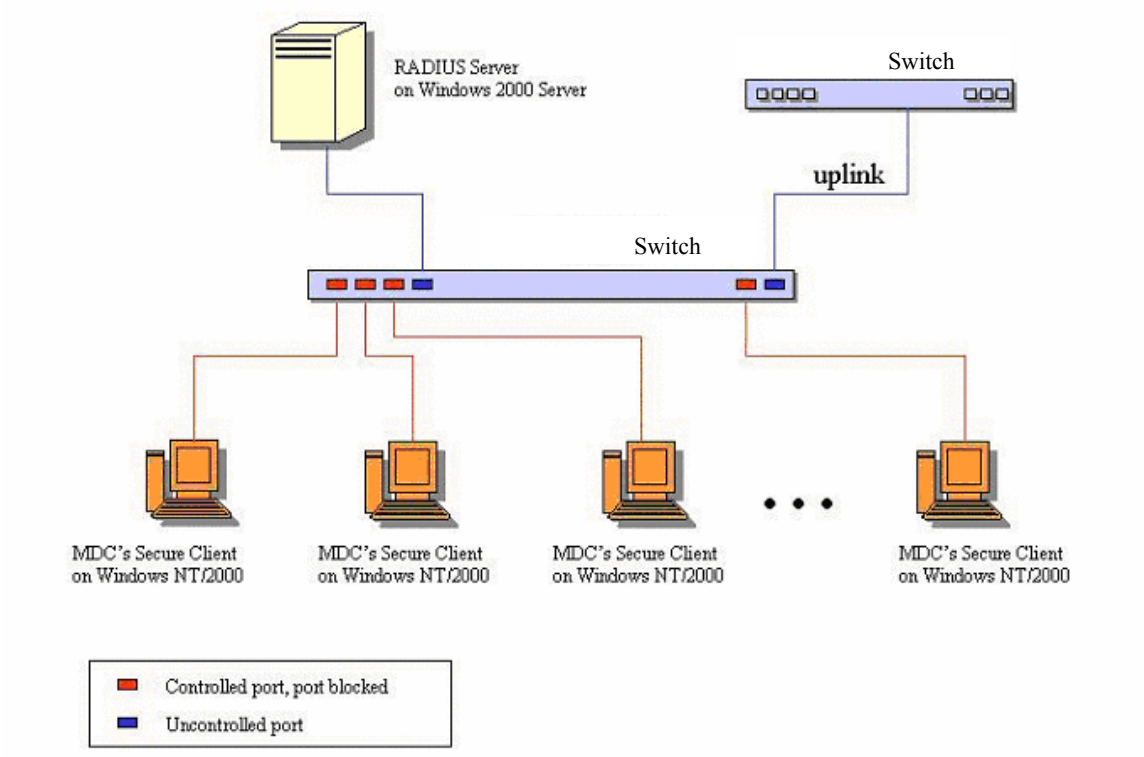


Figure B-26: Typical 802.1x Configuration Prior to User Authentication

Once the user is authenticated, the Switch unblocks the port that is connected to the user as shown in the next figure.

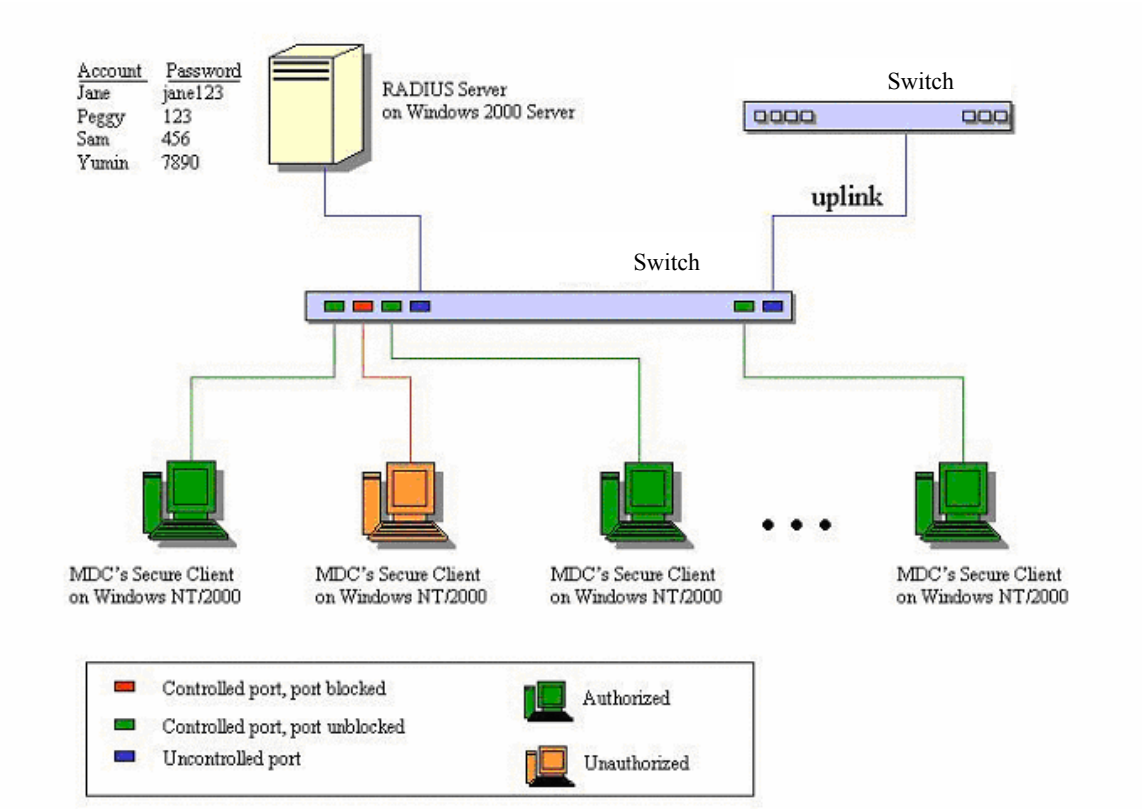


Figure B-27: Typical 802.1x Configuration with User Authentication

The user's information, including account number, password, and configuration details such as IP address and billing information, is stored in a centralized RADIUS server.

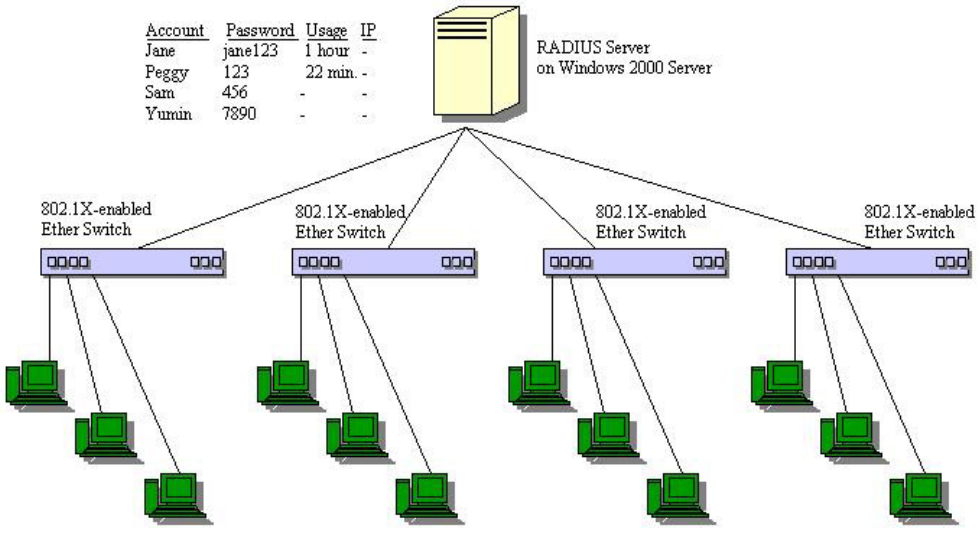


Figure B-28: Typical Configuration with 802.1x Fully Implemented

Table B-1: Conformance to IEEE 802.1x Standards

State Machine Name
Port Timers state machine
Authenticator PAE state machine
The Authenticator Key Transmit state machine
Reauthentication Timer state machine
Backend Authentication state machine
Controlled Directions state machine
The Key Receive state machine

The LFSW-3226L implements the server-side of the **IEEE 802.1x Port-based Network Access Control**. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

IEEE 802.1x operation must be enabled on the switch before it will function. This is done using the **802.1x State** window. 802.1x settings can be configured before being enabled on the switch.

B.8.1. 802.1x State

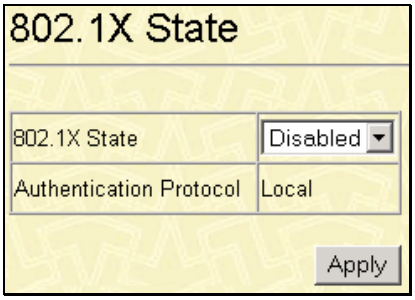


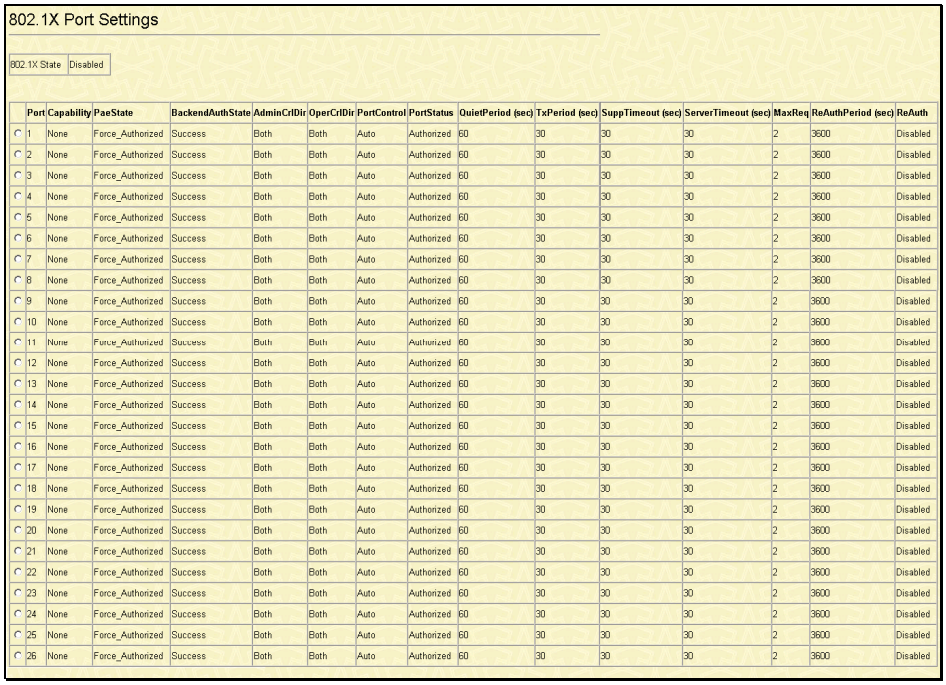
Figure B-29: 802.1x State window

The following fields can be set:

Parameter	Description
802.1x State	This window allows the user to enable or disable the 802.1x Port-Based Network Access control server application on the switch. When the 802.1x function is disabled, authentication packets are flooded to all ports except the source port.

B.8.2. 802.1x Port Settings

Existing 802.1x port settings are displayed and can be configured using the windows below.



802.1X Port Settings

802.1X State: Disabled

	Port	Capability	PaeState	BackendAuthState	AdminCtlDir	OperCtlDir	PortControl	PortStatus	QuietPeriod (sec)	TxPeriod (sec)	SuppTimeout (sec)	ServerTimeout (sec)	MaxReq	ReAuthPeriod (sec)	ReAuth
○	1	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	2	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	3	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	4	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	5	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	6	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	7	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	8	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	9	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	10	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	11	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	12	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	13	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	14	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	15	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	16	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	17	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	18	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	19	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	20	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	21	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	22	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	23	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	24	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	25	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled
○	26	None	Force_Authorized	Success	Both	Both	Auto	Authorized	60	30	30	30	2	3600	Disabled

Figure B-30: 802.1x Port Settings window

Click the radio button on the far left that corresponds to the port you want to configure and click the **Edit** button. 802.1x must be enabled for the **Edit** button to be shown on the **802.1x Port Settings** window. The following window will appear:

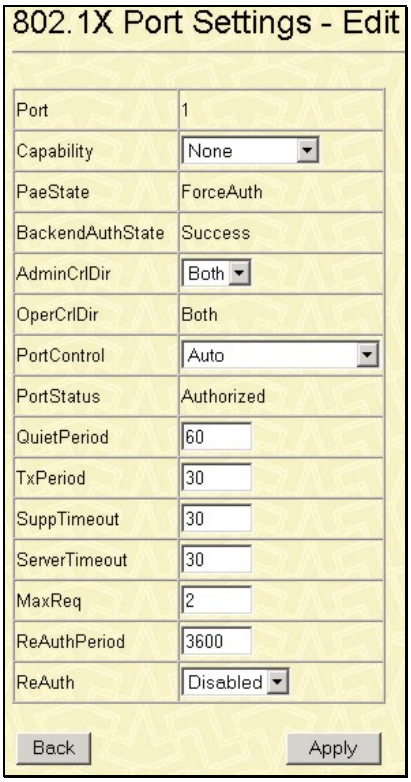


Figure B-31: 802.1x Port Settings – Edit window

Configure the following 802.1x port settings:

Parameter	Description
Capability	Two role choices can be selected: Authenticator – A user must pass the authentication process to gain access to the network. None – The port is not controlled by the 802.1x functions.
PaeState	Shows the current state of the Authenticator.
BackendAuthState	Shows the current state of the Backend Authenticator.
AdminCrlDir	From the pull-down menu, select whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.
OperCrlDir	This displays whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.
Port Control	Displays the administrative control over the port's authorization status. Force_Authorized forces the Authenticator of the port to become Authorized. Force_Unauthorized forces the port to become Unauthorized. Auto means the port state reflects the outcome of the authentication exchange between supplicant, authenticator, and authentication.
PortStatus	Lists the current port status, be it Authorized or Unauthorized.
QuietPeriod (0-65535)	Select the time interval between authentication failure and the start of a new authentication attempt.
TxPeriod (1-65535)	Select the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.

Parameter	Description
SuppTimeout (1-65535)	Select the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.
ServerTimeout (1-65535)	Select the length of time to wait for a response from a RADIUS server.
MaxReq (1-10)	Select the maximum number of times to retry sending packets to the supplicant.
ReAuthPeriod (1-999999999)	Select the time interval between successive re-authentications.
ReAuth	Enable or disable reauthentication.
Port	Port being configured for 802.1x settings.

B.8.3. 802.1X Reauthenticate Ports

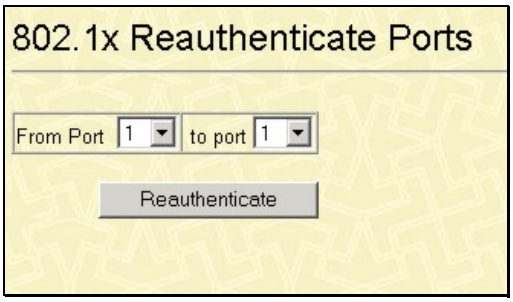


Figure B-32: 802.1X Reauthenticate Ports window

This screen allows you to reauthenticate a port or group of ports. This will allow the user to reauthenticate the device connected with the port. During the reauthentication period, the port status will remain authorized until a failed reauthentication. Choose the port or group of ports using the pull-down menu and click **Reauthenticate** to start the process.

B.8.4. 802.1X Initialize Ports

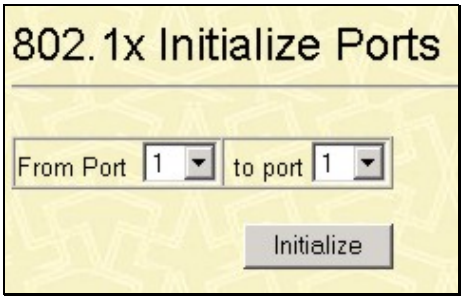


Figure B-33: 802.1X Initialize Ports window.

This window allows you to initialize the authentication state machine of a port or group of ports. Choose the port or group of ports using the pull-down menu and click **Initialize** to start the process.

B.8.5. RADIUS Server Settings

Use this window to configure the settings the switch will use to communicate with a RADIUS server.

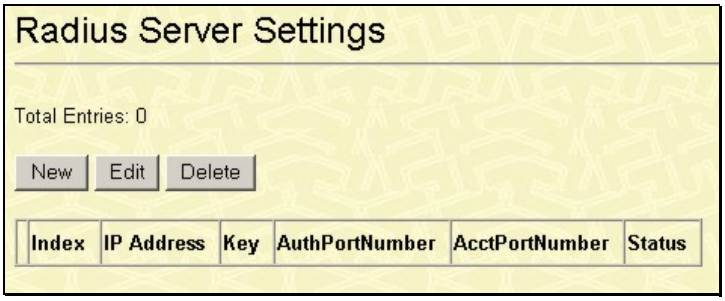


Figure B-34: RADIUS Server Settings window

To add RADIUS server settings click the **New** button and a separate configuration window will appear. To edit an existing RADIUS settings index, select it and click the **Edit** button.

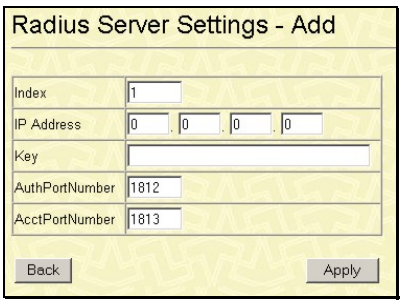


Figure B-35: RADIUS Server Settings – Add window

Configure the following **RADIUS Server Settings** for both the **Add** and **Edit** windows:

Parameter	Description
Index	RADIUS server settings index.
IP Address	Type in the IP address of the RADIUS server.
Key	Type the shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.
AuthPortNumber	Type the UDP port number for authentication requests. The default is 1812.
AcctPortNumber	Type the UDP port number for accounting requests (if an accounting server is being used). The default is 1813.

B.8.6. Local Server User

Figure B-36: 802.1x Local Server User Configuration window

Click **New** to add an **802.1x** local server user:

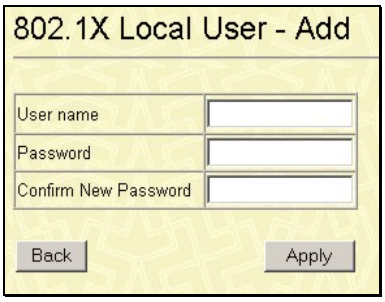


Figure B-37: 802.1x Local User – Add window

B.9. System Log

The switch can send **Syslog** messages to up to four designated servers. Use the **System Log State** to enable this function.

B.9.1. System Log State

Figure B-38: System Log State window

To enable the **System Log Server** settings you have chosen on the **System Log Server** window, select Enabled and click the **Apply** button.

B.9.2. System Log Server

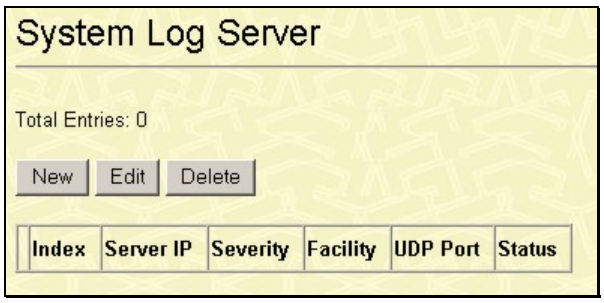


Figure B-39: System Log Server window

Click **New** to add an entry to this table:

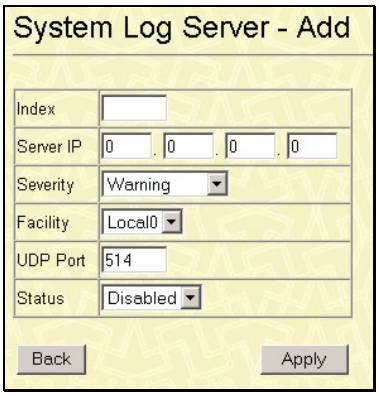


Figure B-40: System Log Server – Add window

Parameter	Description
Index	Syslog server settings index (1-4).
Server IP	Type in the IP address of the Syslog server receiving the message.
Severity	Select the level of message sent, select: Warning, Information or All.

Parameter	Description
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now. Numerical Facility Code 0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog line printer subsystem 7 network news subsystem 8 UUCP subsystem 9 clock daemon 10 security/authorization messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon 16 local use 0 (local0) 17 local use 1 (local1) 18 local use 2 (local2) 19 local use 3 (local3) 20 local use 4 (local4) 21 local use 5 (local5) 22 local use 6 (local6) 23 local use 7 (local7)
UDP Port	Type the UDP port number used for sending Syslog messages. The default is 514.
Status	Choose Enabled or Disabled to activate or deactivate this.

B.10. Multicast Configuration

The Switch supports Multicast configuration. The feature is divided into **IGMP Snooping Global**, **IGMP Snooping Configurations**, and **Static Router Port Settings**.

B.10.1. IGMP Snooping Global

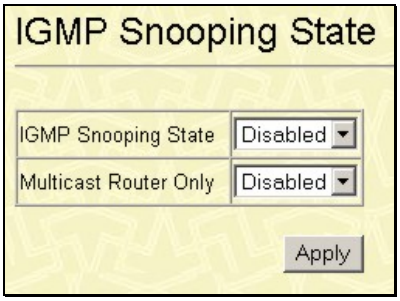


Figure B-41: IGMP Snooping State window

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

B.10.2. IGMP Snooping Configurations

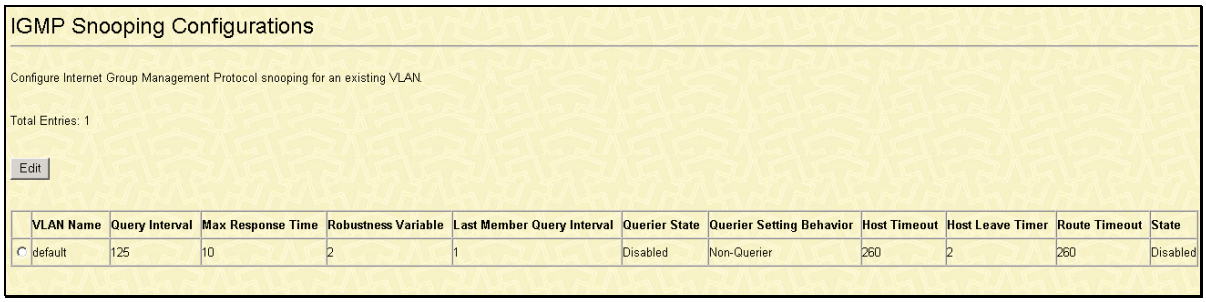


Figure B-42: IGMP Snooping Configurations window

Select the desired IGMP snooping configuration and click **Edit** to open the following window:

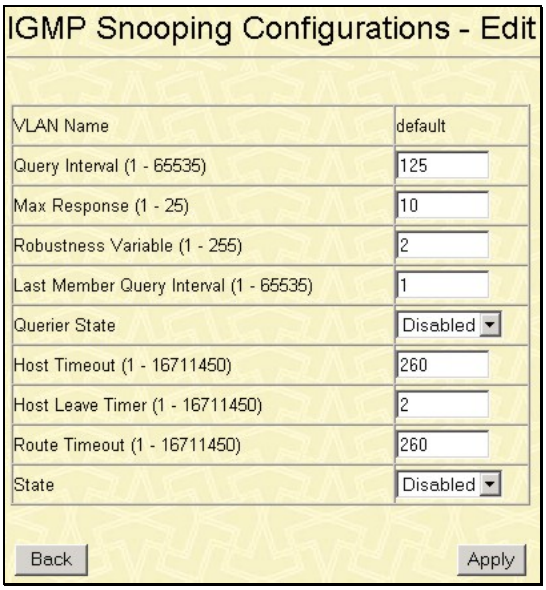


Figure B-43: IGMP Snooping Configurations – Edit window

The following parameters can be set:

Parameter	Description
Query Interval (1-65535)	The time between IGMP queries, set in seconds. The user may set a value between 1 and 65535 seconds. The default is 125 seconds.
Max Response (1-25)	Specifies the maximum amount of time allowed before sending a response report. The user may set a value between 1 and 25 seconds.
Robustness Variable (1-255)	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. The user may wish to increase this value if the subnet loses packets frequently.
Last Member Query Interval (1-65535)	The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The user may lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.
Querier State	This allows the switch to be specified as an IGMP Querier (sends IGMP query packets) or a Non-Querier (does not send IGMP query packets). The user may change the querier state to Enabled or Disabled.
Host Timeout (1 – 16711450)	Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.

Parameter	Description
Host Leave Timer (1 – 16711450)	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted.
Route Timeout (1 – 16711450)	Specifies the maximum amount of time a route will remain in the switch's can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.
State	Enables or disables IGMP Snooping for the chosen VLAN.

B.10.3. Static Router Port Settings

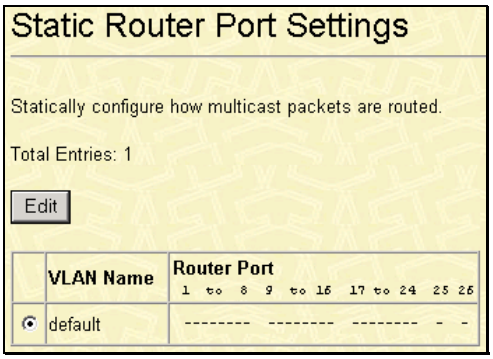


Figure B-44: Static Router Port Settings window

Select an entry and click **Edit** to access the following window:

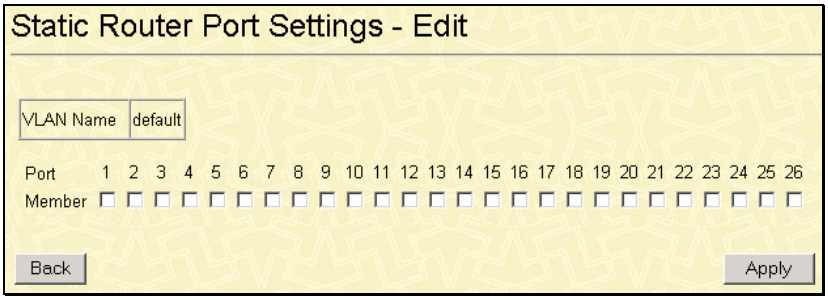


Figure B-45: Static Router Port Settings – Edit window

B.11. SSH Management

SSH is the abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows you to securely login to remote host computers, to execute commands safely in a remote computer and so forth, and to provide secure encrypted and authenticated communications between two non-trusted hosts.

SSH with its array of unmatched security features is an essential tool in today's network environment.

It is a powerful guardian against the numerous security hazards that nowadays threaten network communications.

The Switch's SSH Management windows consist of **SSH State**, **SSH Global**, and **SSH Account Configuration**.

B.11.1. SSH State

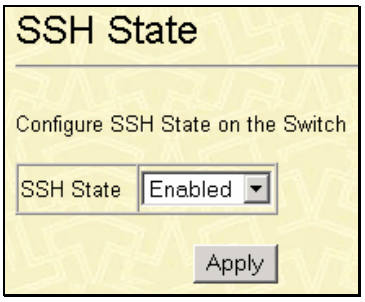


Figure B-46: SSH State window

Toggle **SSH State** to Enabled to implement the Secure Shell protection.

B.11.2. SSH Global

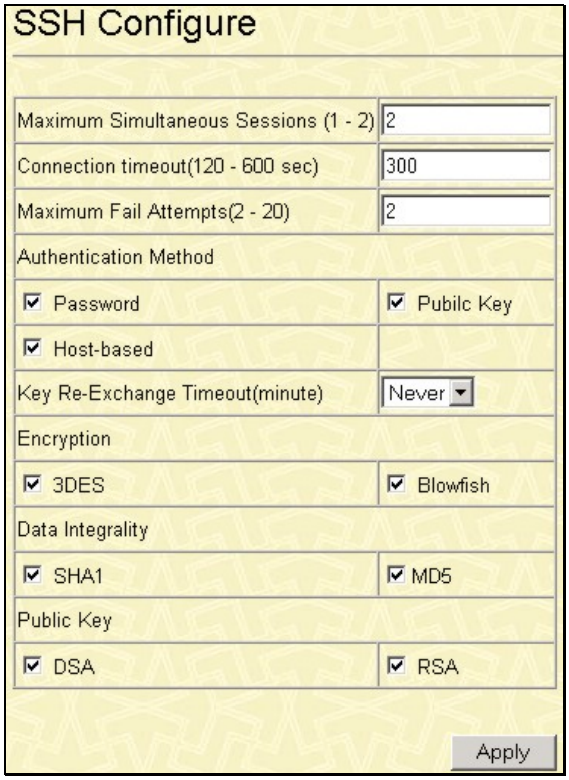


Figure B-47: SSH Configure window

The **SSH Configure** window contains the global server setting: maximum simultaneous sessions, connection timeout, maximum fail attempts, authentication method, key re-exchange timeout, the encryption algorithms, data integrality algorithms and public key algorithms.

The information on the window is described as following:

Parameter	Description
Maximum Simultaneous Sessions (1 – 2)	Specify how many sessions at most the server program will handle simultaneously.
Connection Timeout(120- 600 sec)	Specify how many seconds the connection can survive before the server automatically ends the connection.
Maximum Fail Attempts(2 – 20)	Specify the maximum number of allowed authentication attempts before access is denied.
Authentication Method	Specify the methods of user authentication supported by server.
Key Re-Exchange Timeout(minute)	Use the pull down menu to choose the timeout period for the Key Re-Exchange. The user may choose between Never, 10, 30 or 60 seconds.
Encryption	Specify the algorithm to use for encryption supported by server. 3DES: Use 3DES encryption. Blowfish: Use Blowfish encryption.
Data Integrity	Specify the desired MAC algorithm to use for the data integrity verification. SHA-1: Use the hmac-sha1 MAC. MD5: Use the hmac-md5 MAC.
Public Key	Specify the algorithm to use for the public key. DSA: Use the DSA algorithm. RSA: Use the RSA algorithm.

B.11.3. SSH Account Configuration

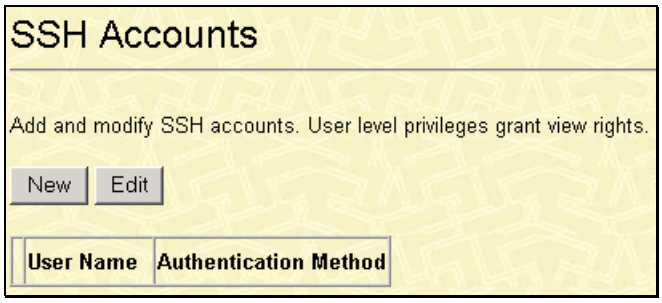


Figure B-48: SSH Accounts window

Click **New** to open the **SSH Accounts – Add** window:

Figure B-49: SSH Accounts – Add window

The **SSH Accounts – Add** window can be used to specify user name, new password, authentication method, host name and host IP.