D-Link ™ DES-3226L

Managed 24-port 10/100Mbps and 2GE ports Layer 2 Ethernet Switch

Manual

Information in this document is subject to change without notice.

Trademarks used in this text: *D-Link* and the *D-LINK* logo are trademarks of D-Link Computer Corporation; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

September 2003 P/N 651S3226L015

FCC Warning

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

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Warning

警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,
在這種情況下使用者會被要求採取某些適當的對策

CONTENTS

Preface

The ***DES-3226L Manual*** is divided into sections that describe the system installation and operating instructions with examples.

Section 1, Introduction - Describes the Switch and its features.

Section 2, Installation– Helps you get started with the basic installation of the Switch and also describes the front panel, rear panel, side panels, and LED indicators of the Switch.

Section 3, Connecting the Switch – Tells how you can connect the Switch to your Ethernet/Fast Ethernet network.

Section 4, Introduction to Switch Management – Talks about Local Console Management via the RS-232 DCE console port and other aspects about how to manage the Switch.

Section 5, Basic Switch Configuration – A detailed discussion about configuring some of the basic functions of the switch, including accessing the Switch information, using the Switch's utilities and setting up network configurations.

Section 6 Advanced Setup – A more detailed discussion of some of the management features of the Switch including, Port Trunk Groups, IEEE 802.1p Priority Queues, VLANs, and 802.1x Port-based Access Control.

Appendix A, Technical Specifications – The technical specifications of the DES-3226L

Appendix B, Cables and Connectors – Describes the RJ-45 receptacle/connector, straight-through and crossover cables and standard pin assignments.

Appendix C, Cable Lengths – Information on cable types and maximum distances.

Glossary – Lists definitions for terms and acronyms used in this document.

Intended Readers

The DES-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

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [**copy *filename***] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
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.
Boldface Typewriter Font	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Italics	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type *filename* means that you should type the actual filename instead of the word shown in italic.
Menu Name > **Menu Option**	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.

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your device.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this safety section, the caution icon (⚠) is used to indicate cautions and precautions that you need to review and follow.

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 practices.

⚠ **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.

⚠ **CAUTION:** 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):

1. 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.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads and an antistatic grounding strap.

SECTION 1

Introduction

Ethernet Technology

Fast Ethernet Technology

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-T, provides a non-disruptive, smooth evolution from 10BASE-T technology.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100Mbps Fast Ethernet and a one hundred-fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet are essential to coping with the network bottlenecks that frequently develop as computers and their busses get faster and more users use applications that generate more traffic. Upgrading key components, such as your backbone and servers to Gigabit Ethernet can greatly improve network response times as well as significantly speed up the traffic between your subnetworks.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur

10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies.

Switching Technology

Another key development pushing the limits of Ethernet technology is in the field of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by making it possible for a local area network to be divided into different *segments*, which are not competing with each other for network transmission capacity, and therefore decreasing the load on each segment.

The switch acts as a high-speed selective bridge between the individual segments. Traffic that needs to go from one segment to another (from one port to another) is automatically forwarded by the switch, without interfering with any other segments (ports). This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

For Fast Ethernet or Gigabit Ethernet networks, a switch is an effective way of eliminating problems of chaining hubs beyond the "two-repeater limit." A switch can be used to split parts of the network into different collision domains, for example, making it possible to expand your Fast Ethernet network beyond the 205-meter network diameter limit for 100BASE-TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks.

Switching LAN technology is a marked improvement over the previous generation of network bridges, which were characterized by higher latencies. Routers have also been used to segment local area networks, but the cost of a router and the setup and maintenance required make routers relatively impractical. Today's switches are an ideal solution to most kinds of local area network congestion problems.

Switch Description

The DES-3226L is equipped with unshielded twisted-pair (UTP) cable ports providing dedicated 10 or 100 Mbps bandwidth. The Switch has 24 UTP ports and Auto MDI-X/MDI-II convertible ports that can be used for uplinking to another switch. These ports can be used for connecting PCs, printers, servers, hubs, routers, switches and other networking devices. 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.

In addition, the Switch has 2 Mini-GBIC combo ports. These two-gigabit combo ports are ideal for connecting to a server or network backbone.

This stand-alone Switch enables the network to use some of the most demanding multimedia and imaging applications concurrently with other user applications without creating bottlenecks. The built-in console interface can be used to configure the Switch's settings for priority queuing, VLANs, and port trunk groups, port monitoring, and port speed.

Features

- IEEE 802.3 10BASE-T compliant
- IEEE 802.3u 100BASE-TX compliant
- IEEE 802.3ab 1000BASE-T compliant
- IEEE 802.3z 1000BASE-LX/SX 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 engine 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
- IGMP Snooping support
- SNMP 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 for connecting to end stations, servers, hubs and other networking devices.
- 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.

Important Note:

For customers interested in D-View, D-Link Corporation's proprietary SNMP management software, go to the D-Link Website (www.dlink.com.cn) and download the software and manual.

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.

DES-3226L

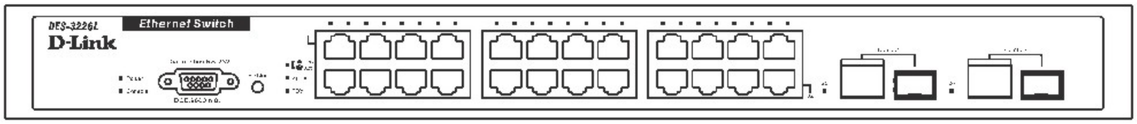


Figure 1- 1. Front Panel View of the DES-3226L as shipped

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 shows the LED indicators for the Switch along with an explanation of each indicator.

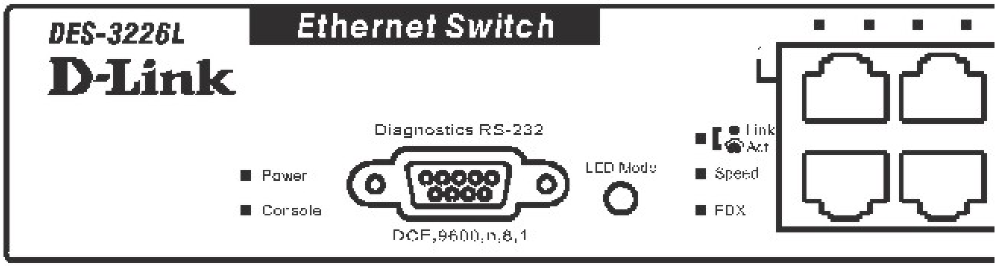


Figure 1- 2. LED Indicators

Power	This LED will light green after the Switch is powered on to indicate the ready state of the device. The indicator is dark when the Switch is powered off.
Console	This LED should blink during the Power-On Self Test (POST). When the POST is finished, the LED goes dark. This LED will light solid amber when the POST test has failed. This indicator is lit sold 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.
Port LEDs	One row of LEDs for each port is located above the ports on the front panel. The first LED is for the top port and the second one is for the bottom port. These LEDs will light accordingly with the Link/Act, Speed and FDX options chosen with the LED Mode button. A description of each is listed below.
Link/Act	When the LED mode has been changed to Link/Act, the LEDs will light steady green to indicate a valid link. A blinking LED indicates activity on the port.
Speed	When the LED mode has been changed to Speed, the LEDs will light steady green to indicate that 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, while an unlit LED indicates a transfer rate of 100Mbps or 10Mbps.
FDX	When the LED mode has been changed to FDX, the LEDs will light steady green to indicate 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.

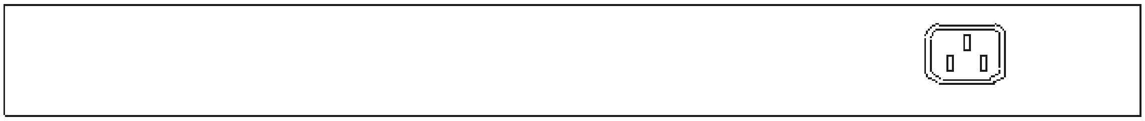


Figure 1- 3. Rear panel view of the Switch

The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. 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. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

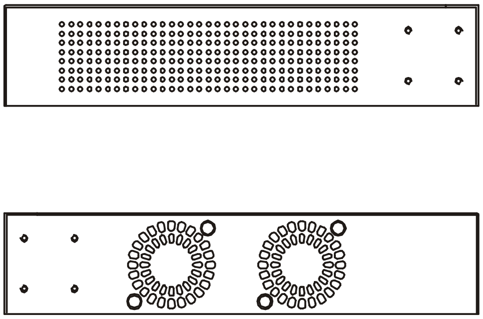


Figure 1-4. Side Panels (the left-hand panel is pictured on top)

Gigabit Combo Ports

In addition to the 24 10/100 Mbps ports, the Switch features two **Gigabit Ethernet Combo** ports. These two ports are 1000BASE-T copper ports (provided) and Mini-GBIC ports (optional). See the diagram below to view the two Mini-GBIC port modules being plugged into the Switch. 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.

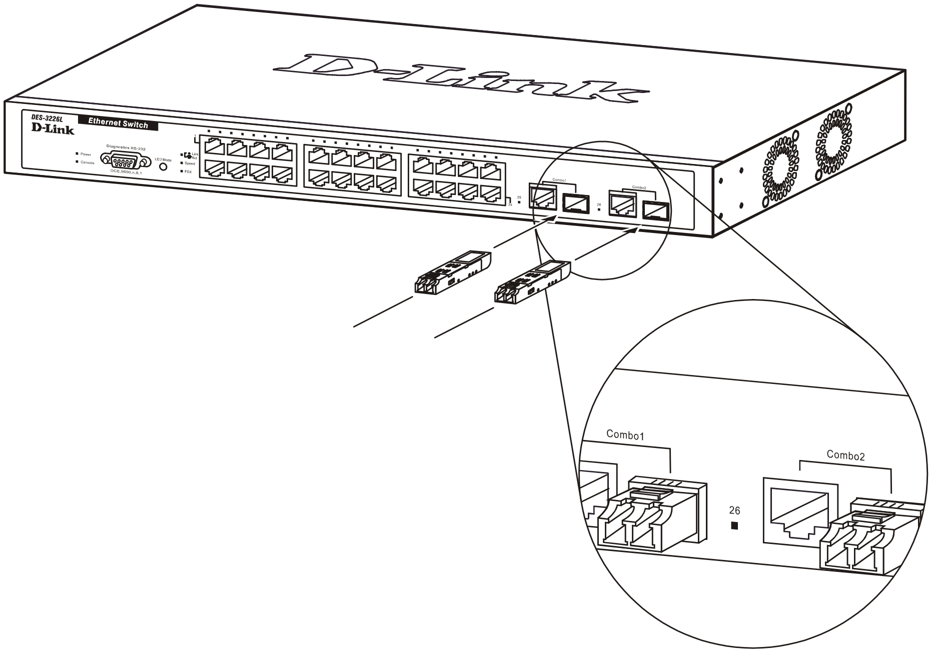


Figure 1- 5. Mini-GBIC modules plug-in to the Switch

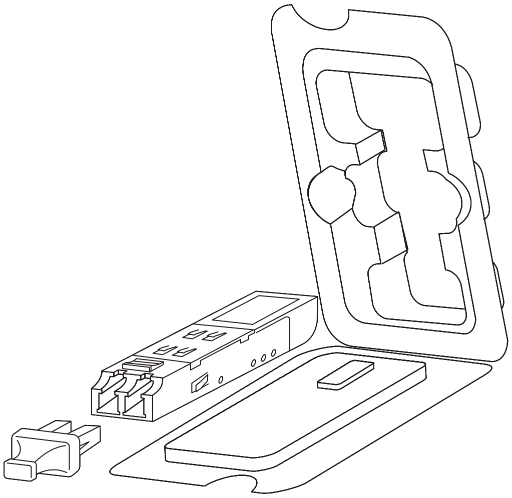


Figure 1- 6. Installing the Mini-GBIC Module

SECTION 2

Installation

Package Contents

Open the shipping carton of the Switch and carefully unpack its contents. The carton should contain the following items:

- One DES-3226L Stand-alone Switch
- One AC power cord
- This Manual
- Registration card
- Mounting kit (two brackets and screws)
- Four rubber feet with adhesive backing
- RS-232 console cable

If any item is found missing or damaged, please contact your local D-Link Reseller for replacement.

Before You Connect to the Network

The site where you install the Switch may greatly affect its performance. Please follow these guidelines for setting up the Switch.

- Install the Switch on a sturdy, level surface that can support at least 3 kg of weight. Do not place heavy objects on the Switch.
- The power outlet should be within 1.82 meters (6 feet) of the Switch.
- Visually inspect the power cord and see that it is fully secured to the AC power port.
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch. Leave at least 10 cm (4 inches) of space at the front and rear of the Switch for ventilation.
- Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.

- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- When installing the Switch on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the Switch, protect the casing from scratches and prevent it from scratching other surfaces.

Installing the Switch Without the Rack

When installing the Switch on a desktop or shelf, the rubber feet included with the Switch should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow enough ventilation space between the Switch and any other objects in the vicinity.

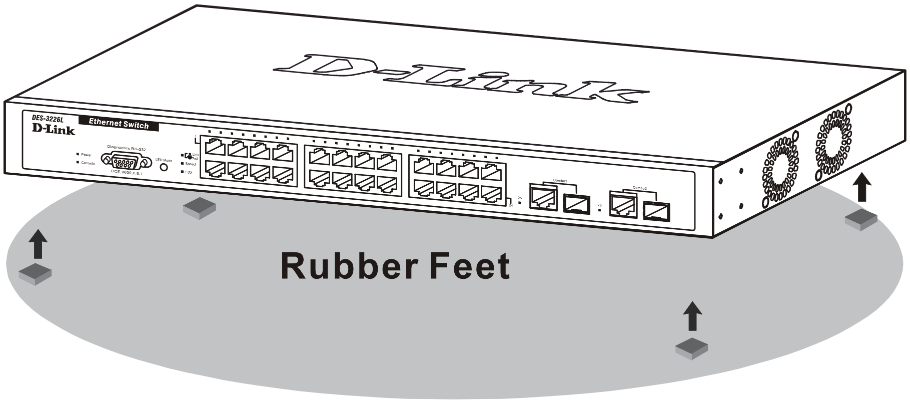


Figure 2- 1. Prepare Switch for installation on a desktop or shelf

Installing the Switch in a Rack

The Switch can be mounted in a standard 19" rack. Use the following diagrams to guide you.

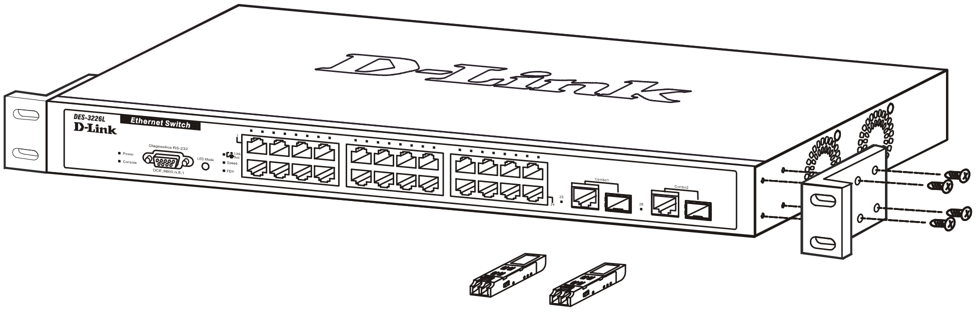


Figure 2- 2. Fasten mounting brackets to Switch

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, you can mount the Switch in a standard rack as shown in Figure 2-3 on the following page.

Mounting the Switch in a standard 19" rack.

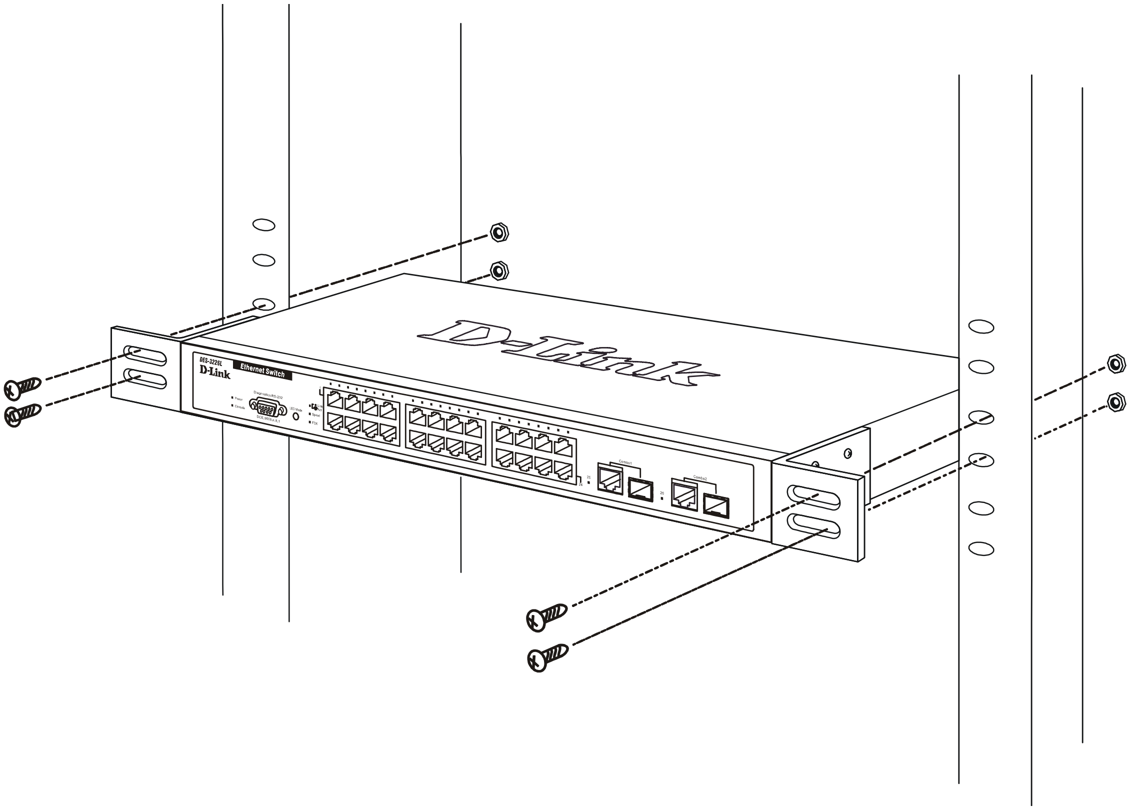


Figure 2- 3. Installing Switch in a rack

Power On

Plug one end of the AC power cord into the power connector of the Switch and the other end into the local power source outlet.

After the Switch is powered on, the LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.

Power Failure

As a precaution, in the event of a power failure, unplug the Switch. When power is resumed, plug the Switch back in.

Section 3

Connecting The Switch

Switch To End Node
Switch To Hub or Switch
Connecting To Network Backbone or Server

NOTE: All 24 high-performance NWay Ethernet ports can support both MDI-II and MDI-X connections.

Switch To End Node

End nodes include PCs outfitted with a 10, 100 or 1000 Mbps RJ-45 Ethernet/Fast Ethernet Network Interface Card (NIC) and most routers.

An end node can be connected to the Switch via a twisted-pair Category 3, 4, or 5 UTP/STP cable. The end node should be connected to any of the ports of the Switch.

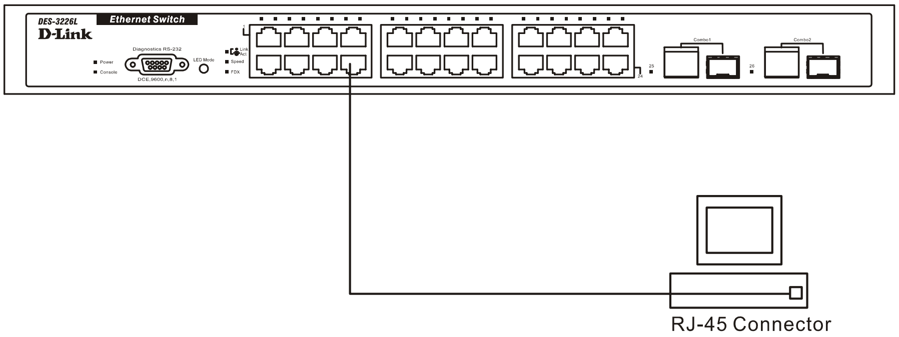


Figure 3- 1.Switch connected to an end node

The **Link/Act** LEDs for each UTP port light green when the link is valid. A blinking LED indicates packet activity on that port.

Switch to Hub or Switch

These connections can be accomplished in a number of ways using a normal cable.

- A 10BASE-T hub or switch can be connected to the Switch via a twisted-pair Category 3, 4 or 5 UTP/STP cable.
- A 100BASE-TX hub or switch can be connected to the Switch via a twisted -pair Category 5 UTP/STP cable.

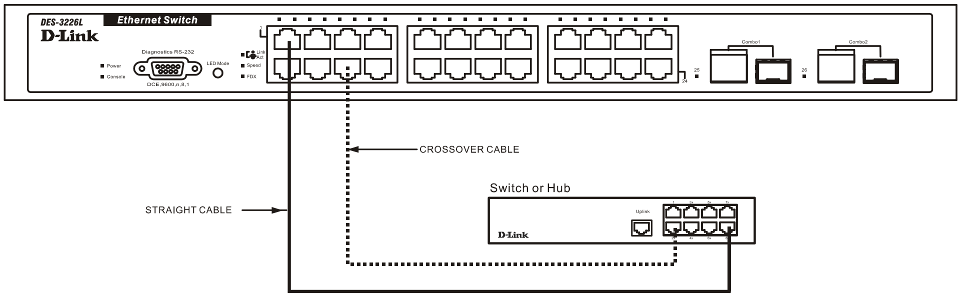


Figure 3- 2 . Switch connected to a port on a hub or switch using either a straight or crossover cable–any normal cable is fine

Connecting To Network Backbone or Server

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.

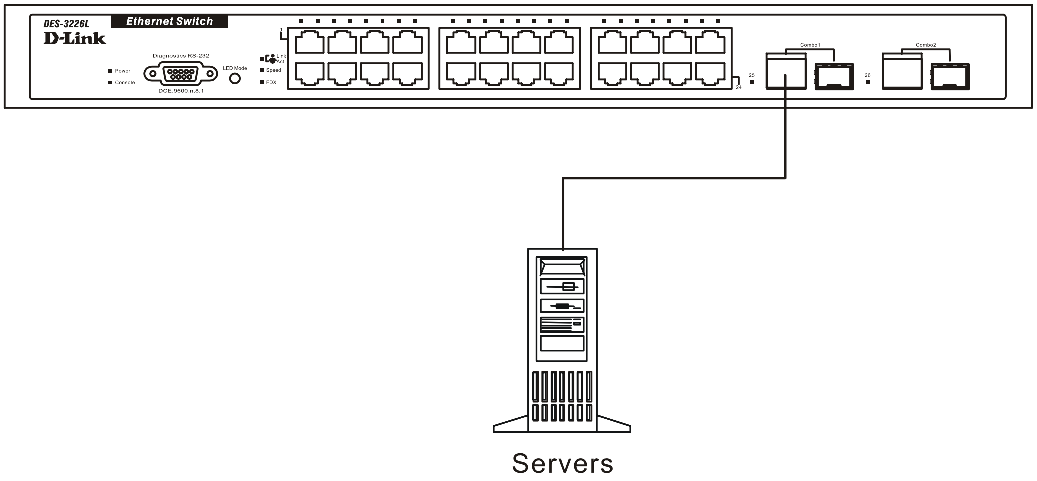


Figure 3- 3. Uplink Connection to a server.

Section 4

Introduction To Switch Management

Management Options

This system may be managed out-of-band through the console port on the front panel or in-band using Telnet. The user may also choose the web-based management, accessible through a web browser.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a web browser, such as Netscape Navigator (version 6.2 and higher) or Microsoft® Internet Explorer (version 5.0).

SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch is supports SNMP version 1.0, version 2.0 and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Command Line Console Interface Through The Serial Port

You can also connect a computer or terminal to the serial console port to access the Switch. The command-line-driven interface provides complete access to all Switch management features.

Connecting the Console Port (RS-232 DCE)

The Switch provides an RS-232 serial port that enables a connection to a computer or terminal for monitoring and configuring the Switch. This port is a female DB-9 connector, implemented as a data terminal equipment (DTE) connection.

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.

To connect a terminal to the console port:

1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
    1. Select the appropriate serial port (COM port 1 or COM port 2).
    3. Set the data rate to 9600 baud.
    4. Set the data format to 8 data bits, 1 stop bit, and no parity.
    5. Set flow control to `none`.
    6. Under **Properties**, select **VT100 for Emulation** mode.
    7. Select **Terminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that you select **Terminal keys** (*not* **Windows keys**).

> ☛ **NOTICE:** 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. See **www.microsoft.com** for information on Windows 2000 service packs.

    8. After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
    9. After the boot sequence completes, the console login screen displays.
    10. If you have not logged into the command line interface (CLI) program, press the Enter key at the User name and password prompts. There is no default user name and password for the Switch. User names and passwords must first be created by the administrator. If you have previously set up user accounts, log in and continue to configure the Switch.

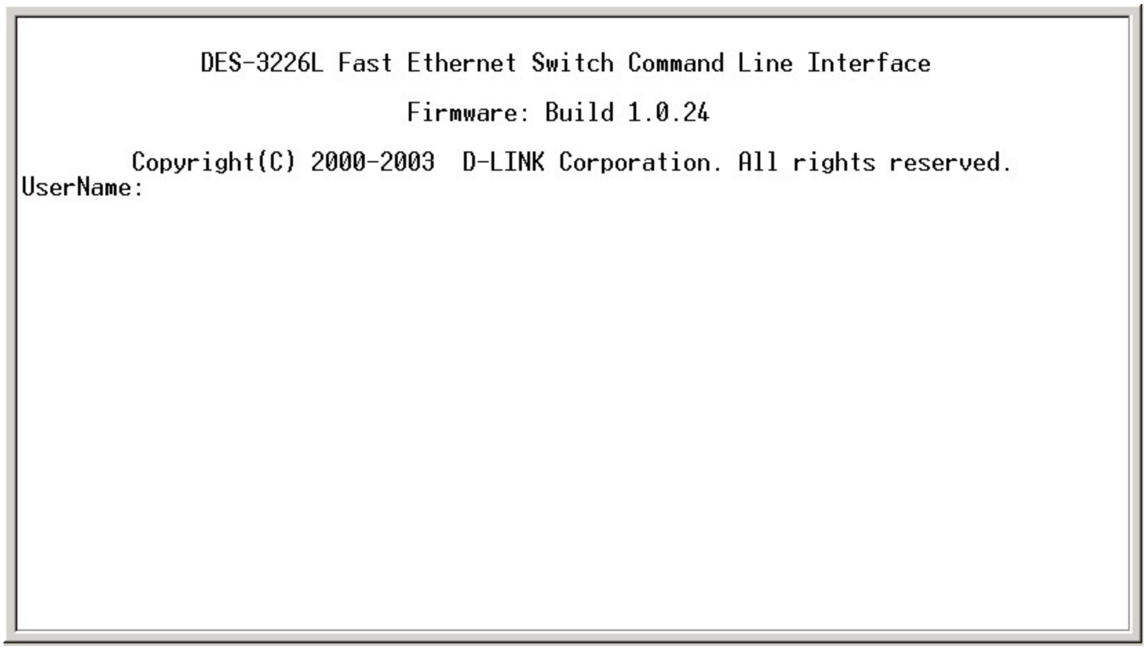
11. Enter the commands to complete your desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the *DES 3226L Command Line Interface Reference Manual* on the documentation CD for a list of all commands and additional information on using the CLI.

When you have completed your tasks, exit the session with the `logout` command or close the emulator program.

Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100. You will be able to set the emulation by clicking on the **File** menu in you HyperTerminal window, clicking on **Properties** in the drop-down menu, and then clicking the **Settings** tab. This is where you will find the **Emulation** options. If you still don't see anything, try rebooting the Switch by disconnecting its power supply.

Once connected to the console, the screen below will appear on your console screen. This is where the user will enter commands to perform all the available management functions. The Switch will prompt the user to enter a user name and a password. Upon the initial connection, there is no user name or password and therefore just press enter twice to access the command line interface.



```
                DES-3226L Fast Ethernet Switch Command Line Interface

                              Firmware: Build 1.0.24

         Copyright(C) 2000-2003  D-LINK Corporation. All rights reserved.
UserName:
```

Figure 4- 1. Initial screen after first connection.

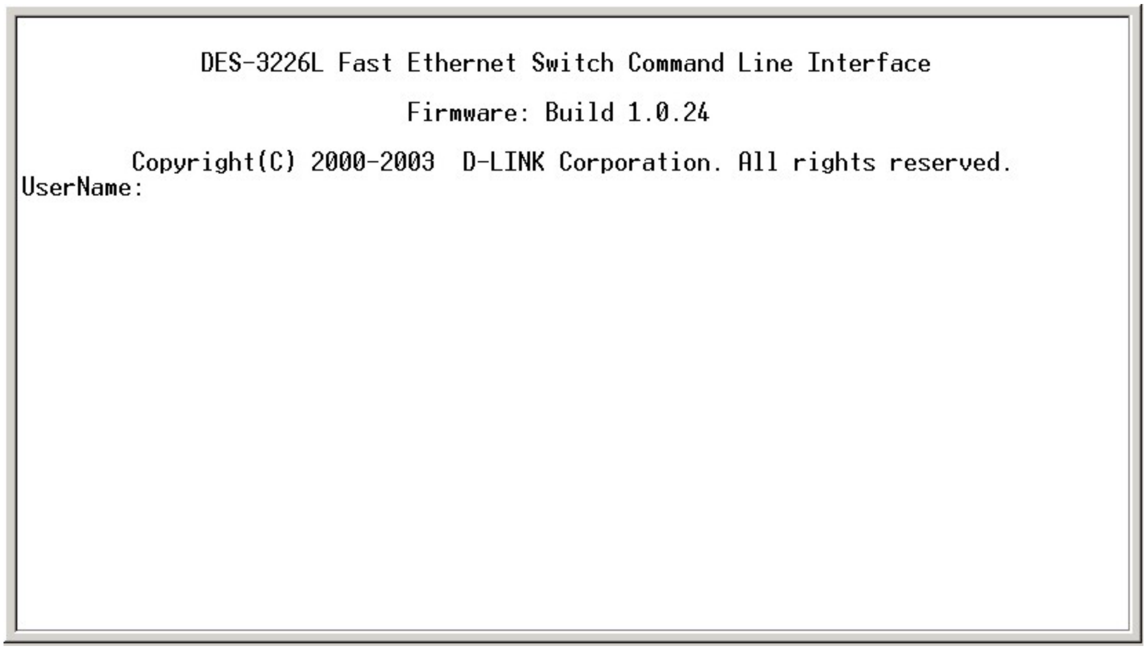
First Time Connecting to The Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch.

NOTE: The passwords used to access the Switch are case-sensitive; therefore, "S" is not the same as "s."

When you first connect to the Switch, you will be presented with the first login screen (shown below).

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.

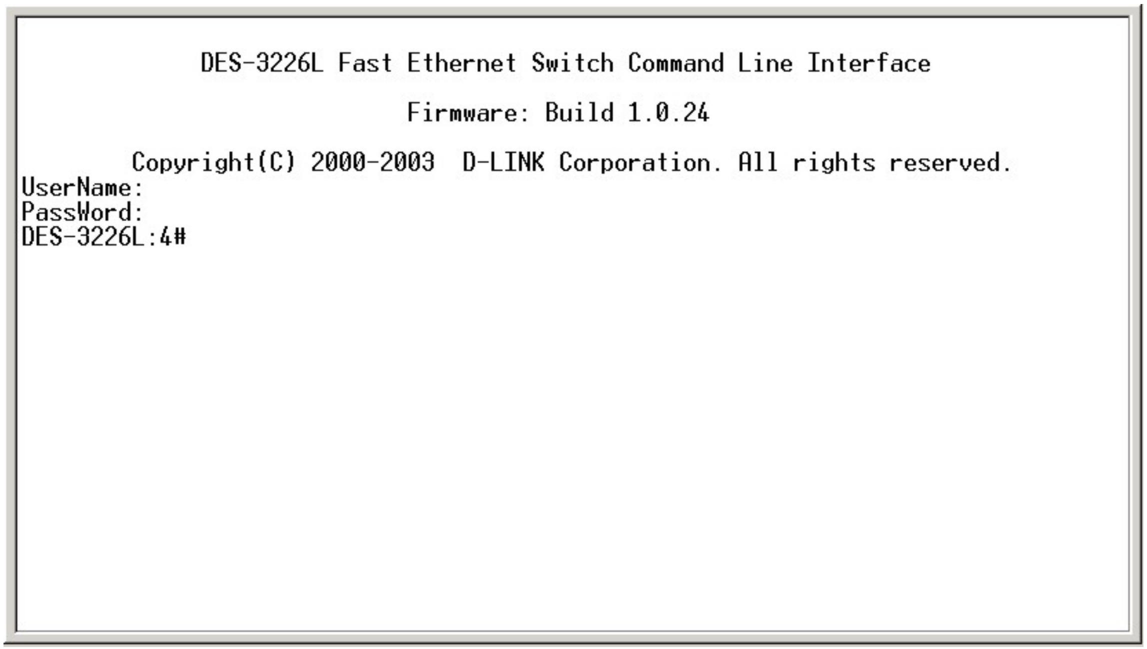


```
             DES-3226L Fast Ethernet Switch Command Line Interface

                          Firmware: Build 1.0.24

        Copyright(C) 2000-2003  D-LINK Corporation. All rights reserved.
UserName:
```

Figure 4- 2. Initial screen, first time connecting to the Switch

Press **Enter** in both the Username and Password fields. You will be given access to the command prompt **DES-3226L** shown below:

There is no initial username or password. Leave the **Username** and **Password** fields blank.



```
                DES-3226L Fast Ethernet Switch Command Line Interface

                               Firmware: Build 1.0.24

         Copyright(C) 2000-2003  D-LINK Corporation. All rights reserved.
UserName:
PassWord:
DES-3226L:4#
```

Figure 4- 3. Command Prompt

The first user automatically gets Admin privileges. It is recommended to create at least one Admin-level user for the Switch.

Password Protection

The DES-3326L does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. If you log in using a predefined administrator-level user name you have privileged access to the Switch's management software.

After your initial login, define new passwords for both default user names to prevent unauthorized access to the Switch, and record the passwords for future reference.

To create an administrator-level account for the Switch, do the following:

1. At the CLI login prompt, enter **create account admin** followed by the <user name> and press the Enter key.
2. You will be asked to provide a password. Type the <password> used for the administrator account being created and press the Enter key.
3. You will be prompted to enter the same password again to verify it. Type the same password and press the Enter key.
4. Successful creation of the new administrator account will be verified by a **Success** message.

User names and passwords can be up to 15 characters in length.

NOTE: Passwords are case sensitive.

The sample below illustrates a successful creation of a new administrator-level account with the user name "newmanager".

```
DES-3226L:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:********
Enter the new password again for confirmation:********
 Success.

DES-3226L:4#
```

NOTICE: CLI configuration commands only modify the running configuration file and are not saved when the Switch is rebooted. To save all your configuration changes in nonvolatile storage, you must use the **save** command to copy the running configuration file to the startup configuration.

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. 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.

The DES-3326L supports SNMP versions 1, 2c, and 3. You can specify which version of SNMP you want to use 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.

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.

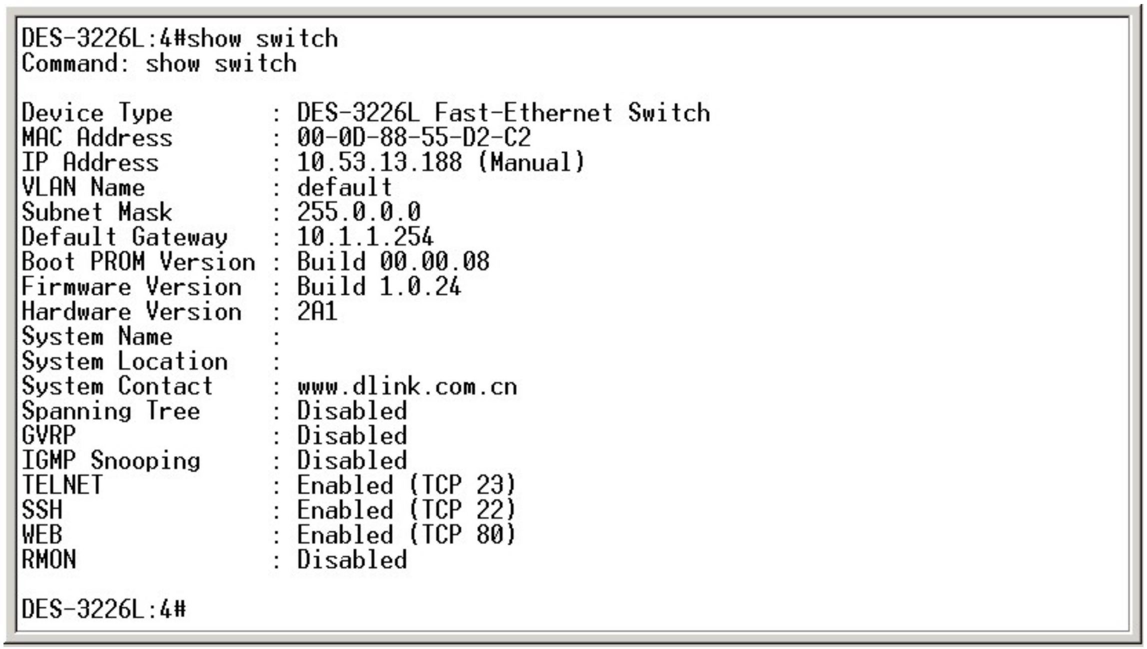
MIBs

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.

IP Address Assignment

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "show switch" into the command line interface, as shown below.



```
DES-3226L:4#show switch
Command: show switch

Device Type       : DES-3226L Fast-Ethernet Switch
MAC Address       : 00-0D-88-55-D2-C2
IP Address        : 10.53.13.188 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 10.1.1.254
Boot PROM Version : Build 00.00.08
Firmware Version  : Build 1.0.24
Hardware Version  : 2A1
System Name       :
System Location   :
System Contact    : www.dlink.com.cn
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
TELNET            : Enabled (TCP 23)
SSH               : Enabled (TCP 22)
WEB               : Enabled (TCP 80)
RMON              : Disabled

DES-3226L:4#
```

Figure 4- 4. Show switch command

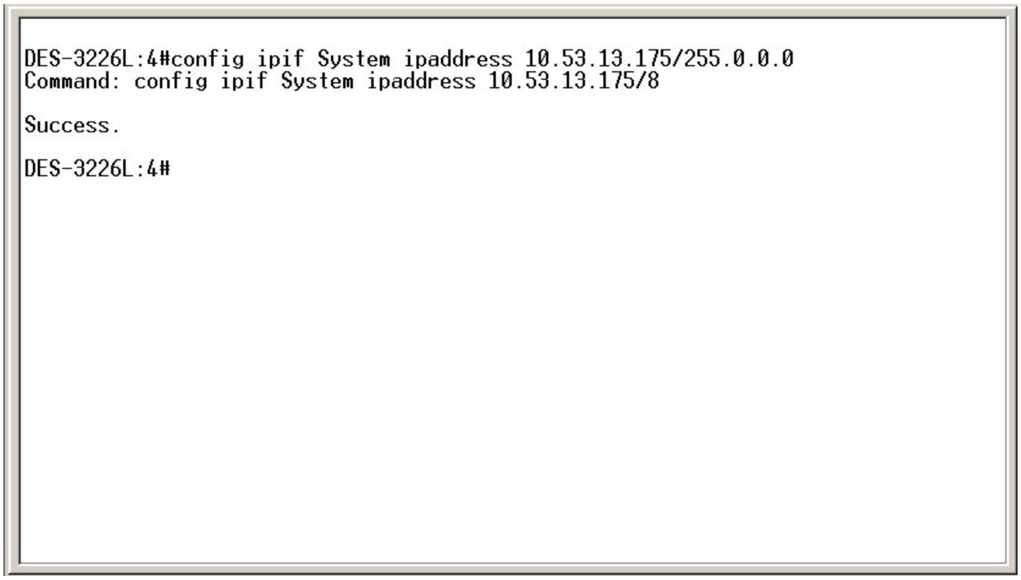
The Switch's MAC address can also be found from the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
2. Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

The IP interface named **System** on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.



```
DES-3226L:4#config ipif System ipaddress 10.53.13.175/255.0.0.0
Command: config ipif System ipaddress 10.53.13.175/8

Success.

DES-3226L:4#
```

Figure 4- 5. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.175 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

Connecting Devices to the Switch

After you assign IP addresses to the Switch, you can connect devices to the Switch.

To connect a device to an SFP transceiver port:

1. Use your cabling requirements to select an appropriate SFP transceiver type.
2. Insert the SFP transceiver (sold separately) into the SFP transceiver slot.
3. Use the appropriate network cabling to connect a device to the connectors on the SFP transceiver.

NOTICE: When the SFP transceiver acquires a link, the associated integrated 10/100/1000BASE-T port is disabled.

Section 5

Introduction to Web-based Switch Configuration

Introduction

All software function of the DES-3226L 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 such as Netscape Navigator/Communicator or Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Login to Web Manager

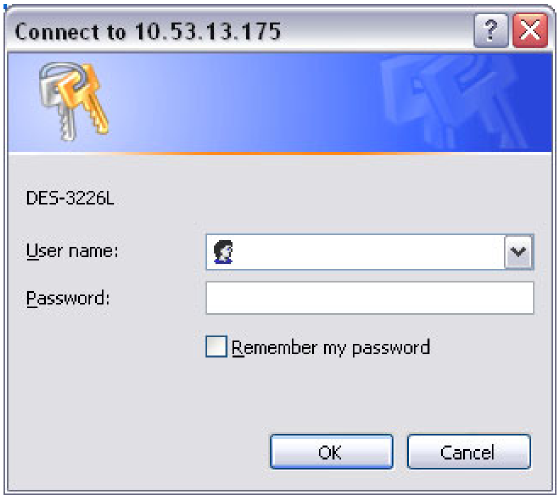
To begin managing your Switch simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

NOTE: The Factory default IP address for the switch is 10.90.90.90.

In the page that opens, click on the **Login to make a setup** button:

Figure 5- 1. Login Button

This opens the management module's user authentication window, as seen below.


Connect to 10.53.13.175

DES-3226L

User name:

Password:

□ Remember my password

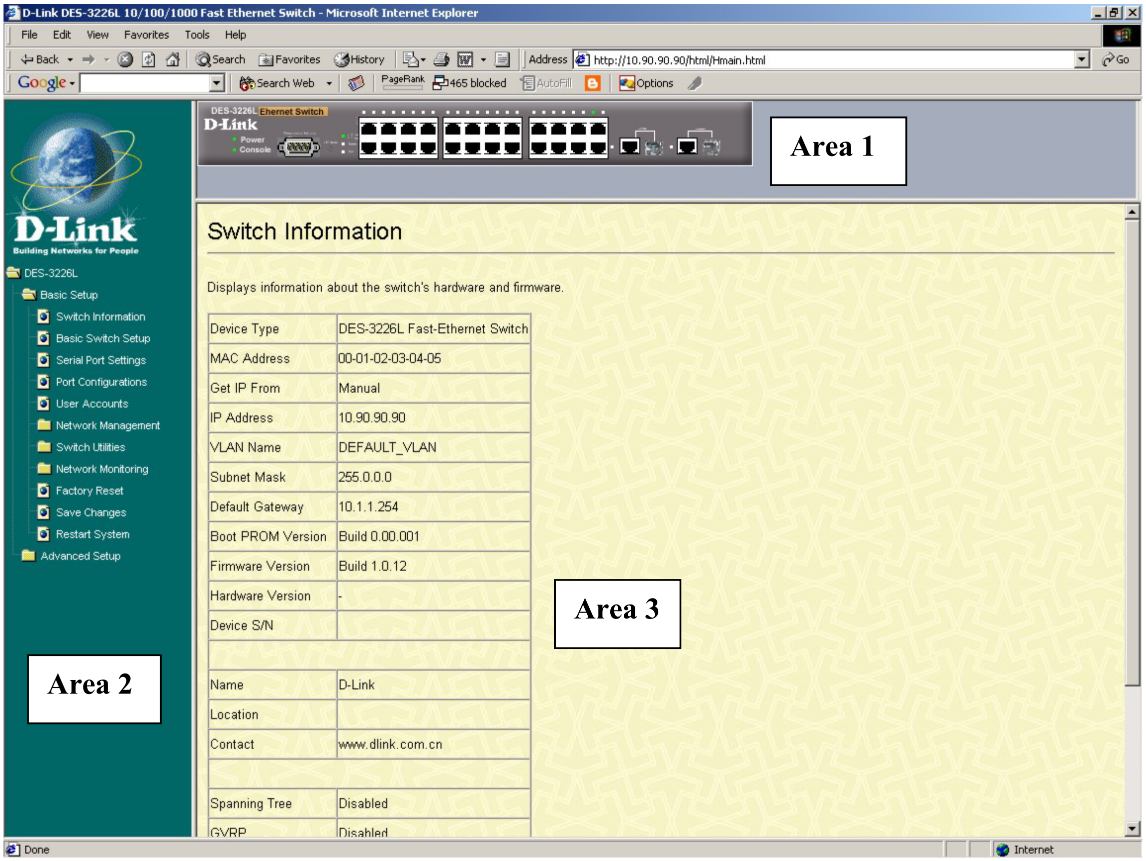
Leave both the **User Name** field and the **Password** field blank and click OK. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into 3 distinct areas as described in the table.



Switch Information

Displays information about the switch's hardware and firmware.

Device Type	DES-3226L Fast-Ethernet Switch
MAC Address	00-01-02-03-04-05
Get IP From	Manual
IP Address	10.90.90.90
VLAN Name	DEFAULT_VLAN
Subnet Mask	255.0.0.0
Default Gateway	10.1.1.254
Boot PROM Version	Build 0.00.001
Firmware Version	Build 1.0.12
Hardware Version	-
Device S/N	
Name	D-Link
Location	
Contact	www.dlink.com.cn
Spanning Tree	Disabled
GVRP	Disabled

Figure 5- 2. Main Web-Manager Screen

Area	Function
1	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including port configuration.
2	Select the menu or window to be displayed. The folder icons can be opened to display the hyperlinked menu buttons and subfolders contained within them. Click the D-Link logo to go to the D-Link website.
3	Presents switch information based on your selection and the entry of configuration data.

NOTICE: Any changes made to the Switch configuration during the current session must be saved in the **Save Changes** web menu (explained below) or use the command line interface (CLI) command **save.**

Web Pages

When you connect to the management mode of the Switch with a web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list and description of the main folders available in the web interface:

Basic Setup: includes screens for *Switch Information, Basic Switch Setup, Serial Port Settings, Port Configurations, User Accounts, Network Management, Switch Utilities, Network Monitoring, Factory Reset, Save Changes* and *Restart System*.

Advanced Setup: includes screens for *Spanning Tree, Forwarding, Configure QoS, Mirroring Configurations, VLAN Configurations, Link Aggregation, 802.1x, System Log, Multicast Configurations* and *SSH Management.*

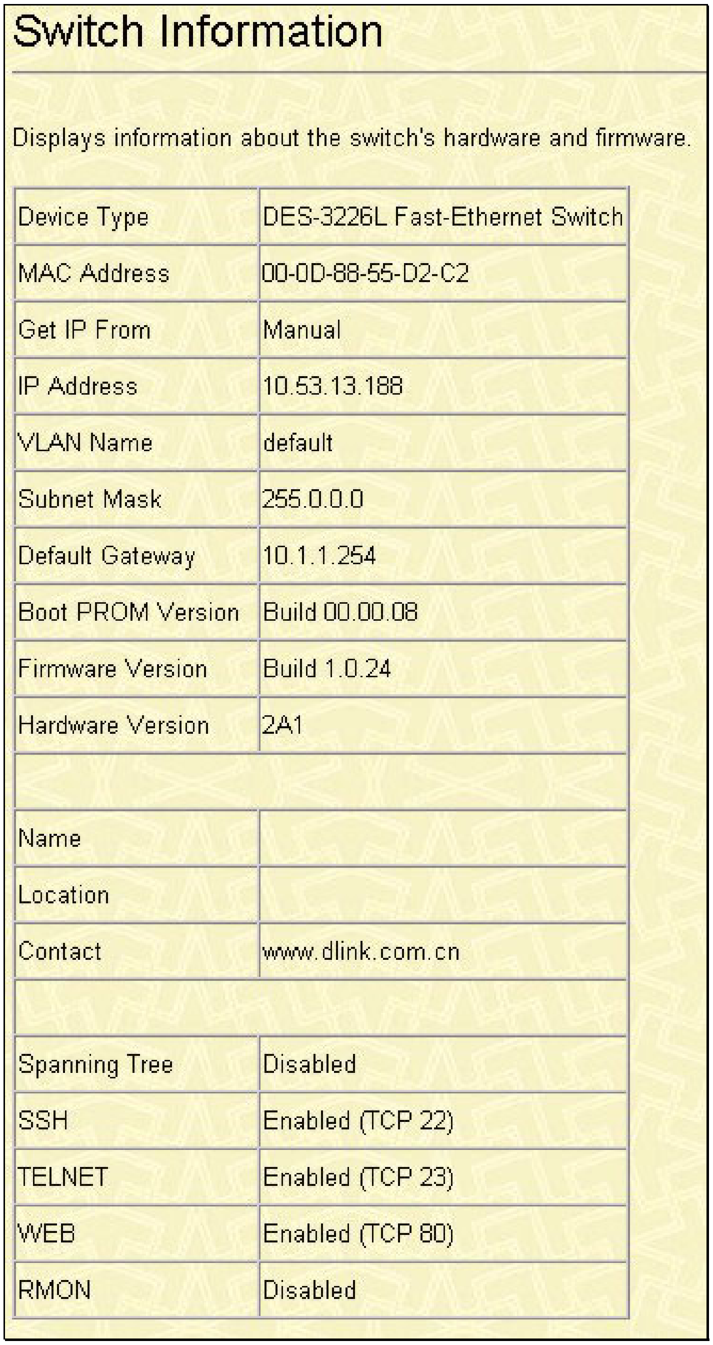
NOTE: Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

Basic Setup

The subsections below describe 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.

Switch Information

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



Switch Information

Displays information about the switch's hardware and firmware.

Device Type	DES-3226L Fast-Ethernet Switch
MAC Address	00-0D-88-55-D2-C2
Get IP From	Manual
IP Address	10.53.13.188
VLAN Name	default
Subnet Mask	255.0.0.0
Default Gateway	10.1.1.254
Boot PROM Version	Build 00.00.08
Firmware Version	Build 1.0.24
Hardware Version	2A1
Name	
Location	
Contact	www.dlink.com.cn
Spanning Tree	Disabled
SSH	Enabled (TCP 22)
TELNET	Enabled (TCP 23)
WEB	Enabled (TCP 80)
RMON	Disabled

Figure 5- 3. Switch Information – Basic Settings

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.

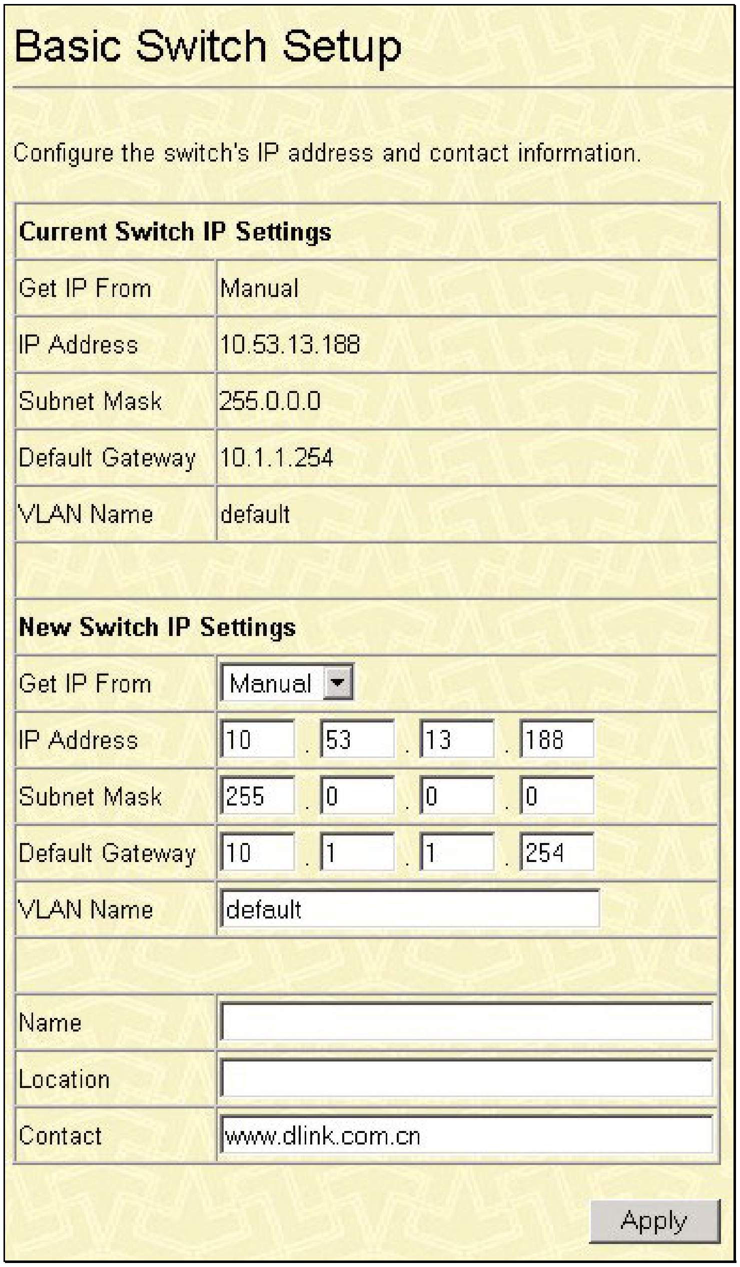
Basic Switch Setup

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:

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.



Basic Switch Setup

Configure the switch's IP address and contact information.

Current Switch IP Settings	
Get IP From	Manual
IP Address	10.53.13.188
Subnet Mask	255.0.0.0
Default Gateway	10.1.1.254
VLAN Name	default
New Switch IP Settings	
Get IP From	Manual ▾
IP Address	10 . 53 . 13 . 188
Subnet Mask	255 . 0 . 0 . 0
Default Gateway	10 . 1 . 1 . 254
VLAN Name	default
Name	
Location	
Contact	www.dlink.com.cn

Figure 5- 4. Basic Switch Setup window

NOTE: the Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

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.

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: <Manual>** 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:

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.
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.

Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

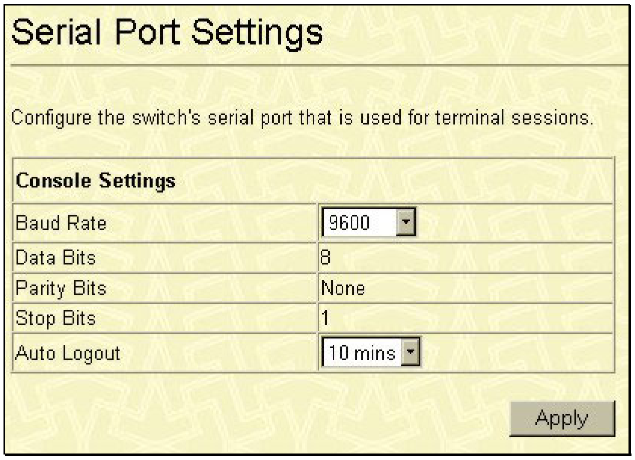
Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

The IP interface named **System** on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

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.



Serial Port Settings

Configure the switch's serial port that is used for terminal sessions.

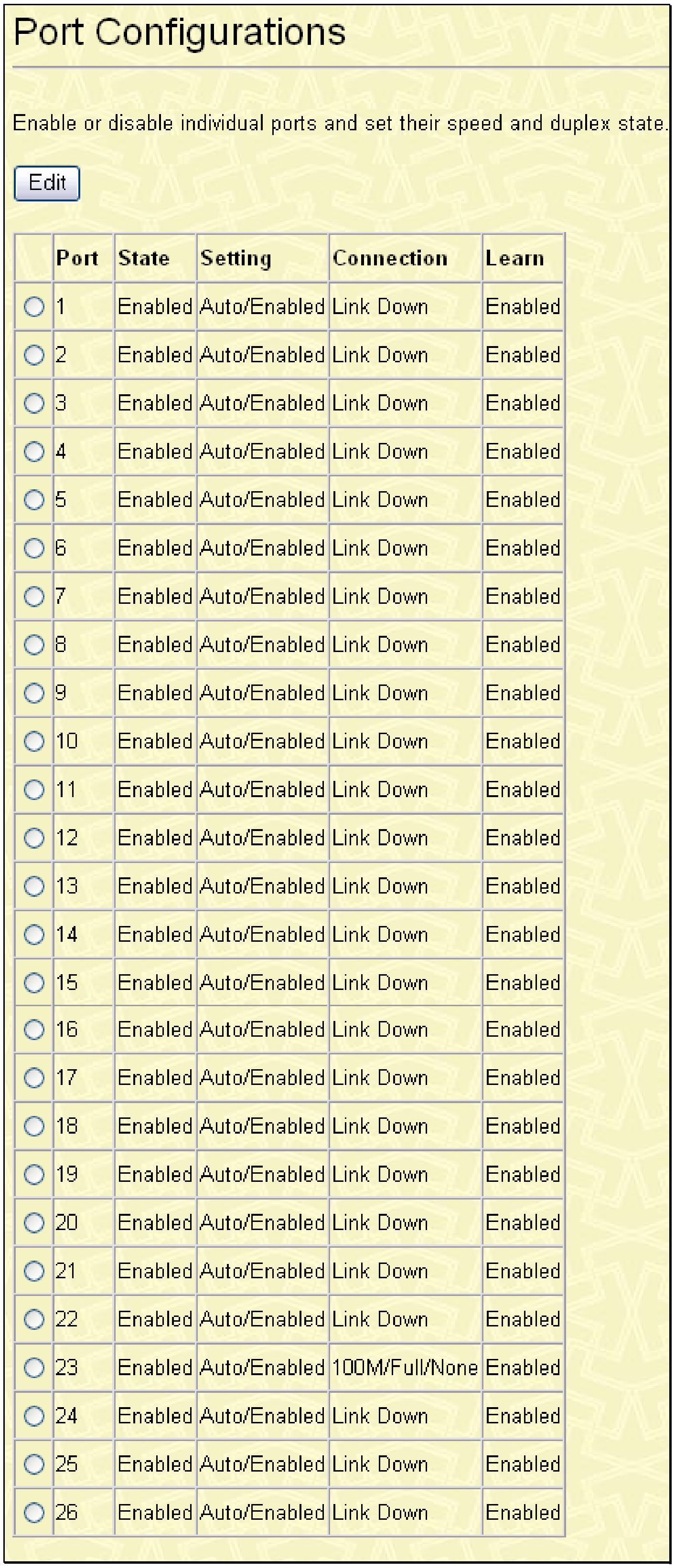
Console Settings	
Baud Rate	9600
Data Bits	8
Parity Bits	None
Stop Bits	1
Auto Logout	10 mins

Figure 5- 5. 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. The **Data Bits (8), Parity Bits (none)** and **Stop Bits (1)** 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.

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.



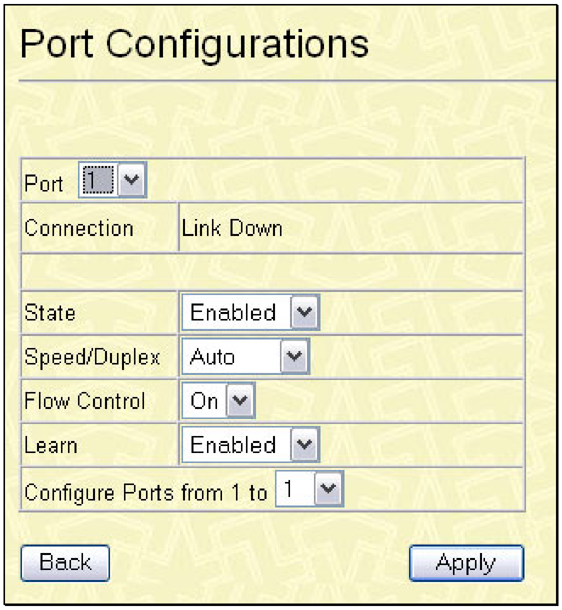
Port Configurations

Enable or disable individual ports and set their speed and duplex state.

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

Figure 5- 6. Port Configurations window

To edit a specific port’s settings, click the corresponding radio button of the port and click **Edit**, which will reveal the following window.



Port Configurations

Port: 1

Connection: Link Down

State: Enabled

Speed/Duplex: Auto

Flow Control: On

Learn: Enabled

Configure Ports from 1 to 1

Figure 5- 7. 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.

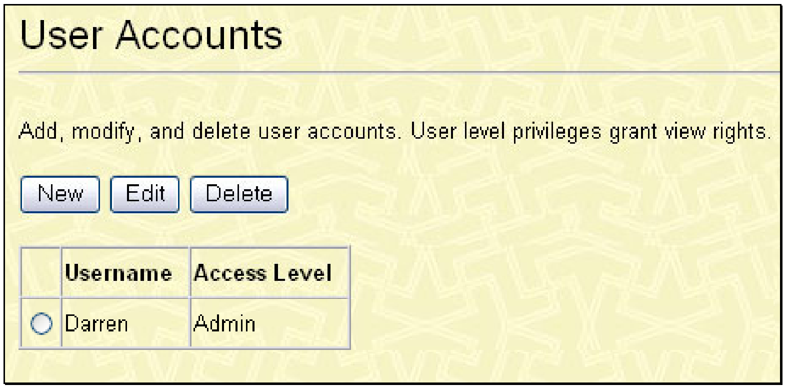
This window allows the user to set the following fields:

Field	Description
Port	Using the pull down menu, select the port you wish to configure.
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** <*Auto*> 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.

User Accounts

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



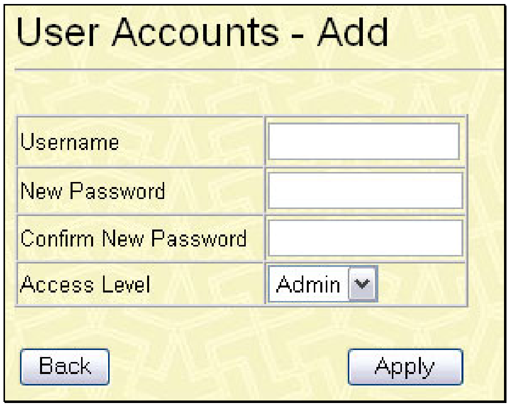
User Accounts

Add, modify, and delete user accounts. User level privileges grant view rights.

	Username	Access Level
○	Darren	Admin

Figure 5- 8. User Accounts Window

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



User Accounts - Add

Username	
New Password	
Confirm New Password	
Access Level	Admin

Figure 5- 9. User Accounts – Add window

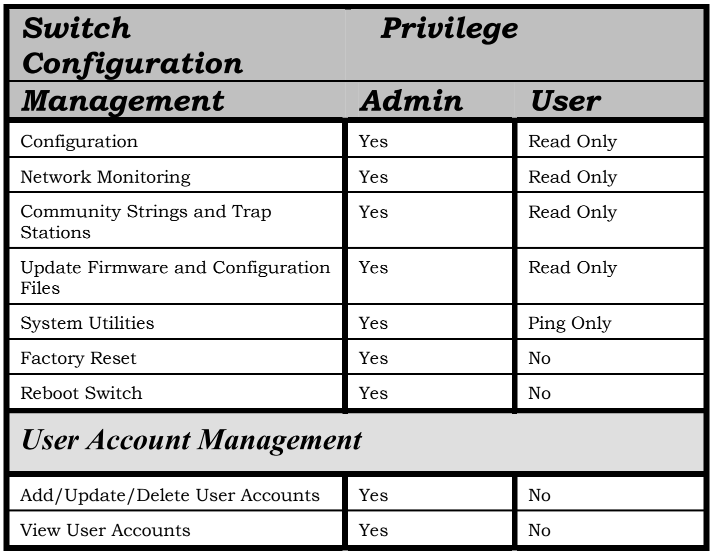
1. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have *Admin* or *User* privileges.
2. Click **Apply** to make the user addition effective.

3. 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.
4. 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.

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**.

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:



Switch Configuration	***Privilege***	
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

Figure 5- 10. Admin and User Privileges

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.

Network Management

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

SNMPv3

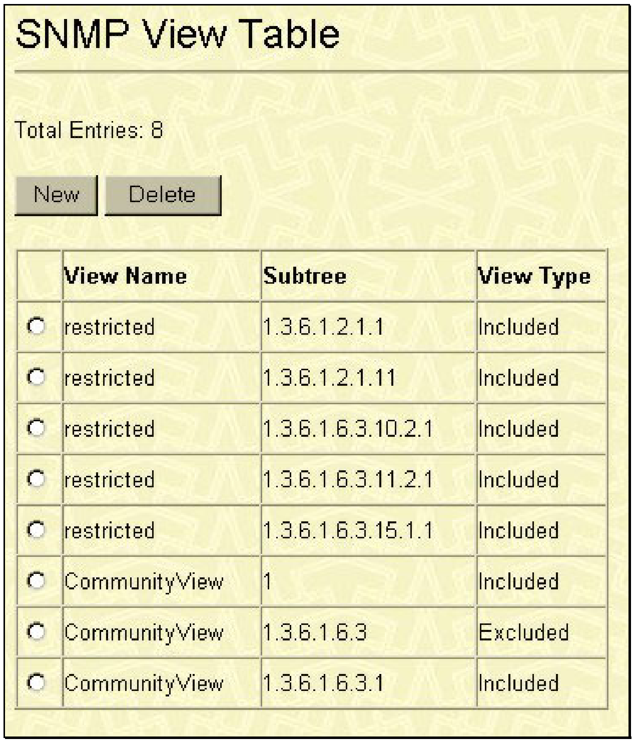
The DES-3226L incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The DES-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**.



Total Entries: 8

	View Name	Subtree	View Type
○	restricted	1.3.6.1.2.1.1	Included
○	restricted	1.3.6.1.2.1.11	Included
○	restricted	1.3.6.1.6.3.10.2.1	Included
○	restricted	1.3.6.1.6.3.11.2.1	Included
○	restricted	1.3.6.1.6.3.15.1.1	Included
○	CommunityView	1	Included
○	CommunityView	1.3.6.1.6.3	Excluded
○	CommunityView	1.3.6.1.6.3.1	Included

Figure 5- 11. 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.

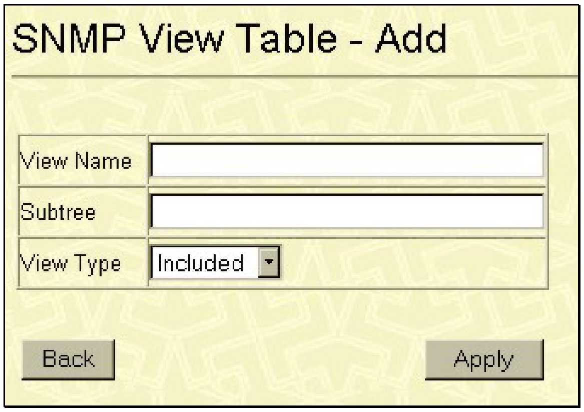


Figure 5- 12. SNMP View Table – Add window

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

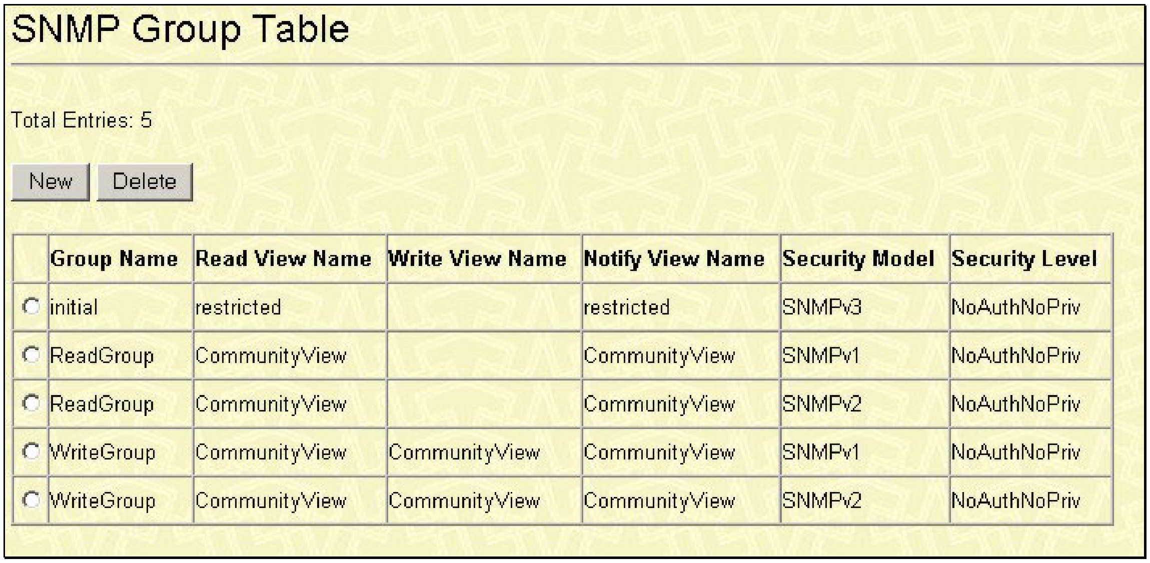
The following parameters can be set:

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**.



SNMP Group Table

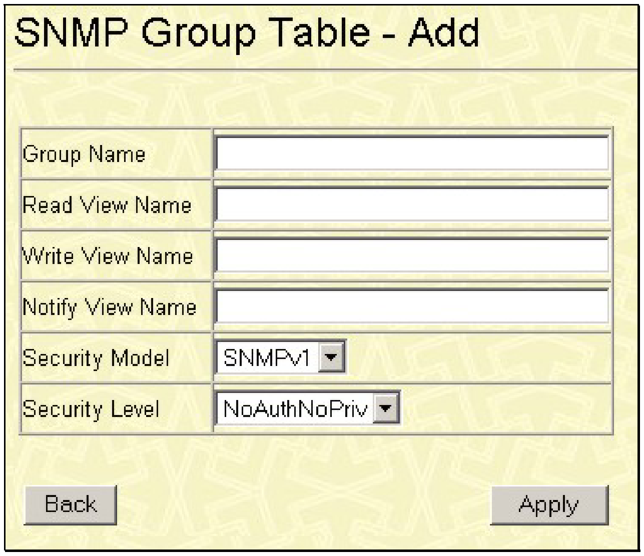
Total Entries: 5

	Group Name	Read View Name	Write View Name	Notify View Name	Security Model	Security Level
○	initial	restricted		restricted	SNMPv3	NoAuthNoPriv
○	ReadGroup	CommunityView		CommunityView	SNMPv1	NoAuthNoPriv
○	ReadGroup	CommunityView		CommunityView	SNMPv2	NoAuthNoPriv
○	WriteGroup	CommunityView	CommunityView	CommunityView	SNMPv1	NoAuthNoPriv
○	WriteGroup	CommunityView	CommunityView	CommunityView	SNMPv2	NoAuthNoPriv

Figure 5- 13. 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 Configuration** page, as shown below.



SNMP Group Table - Add

Group Name	
Read View Name	
Write View Name	
Notify View Name	
Security Model	SNMPv1
Security Level	NoAuthNoPriv

Figure 5- 14. 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.

USM – (User-based Security Module) 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.

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.

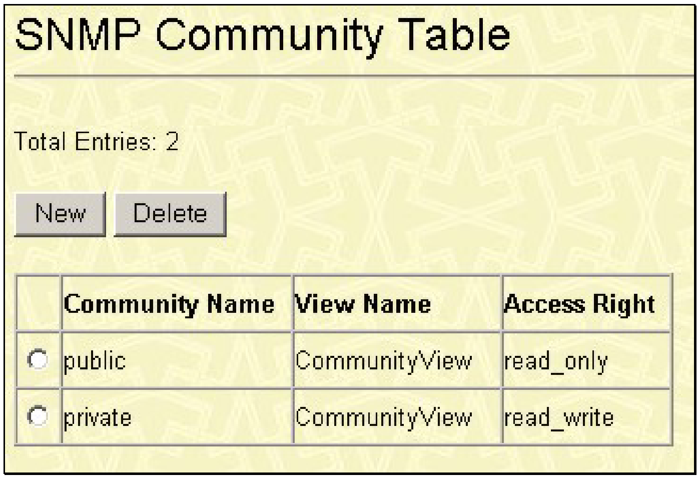
AuthPriv – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

SNMP Community Table Configuration

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**.



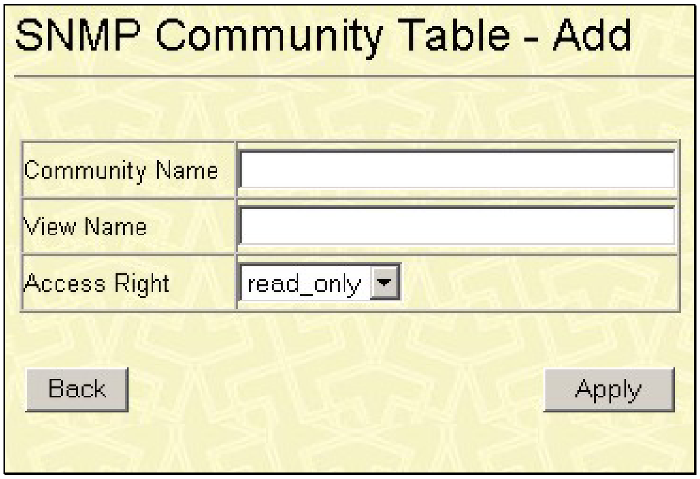
SNMP Community Table

Total Entries: 2

	Community Name	View Name	Access Right
○	public	CommunityView	read_only
○	private	CommunityView	read_write

Figure 5- 15. 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.



SNMP Community Table - Add

Community Name	
View Name	
Access Right	read_only

Figure 5- 16. SNMP Community Table – Add

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.

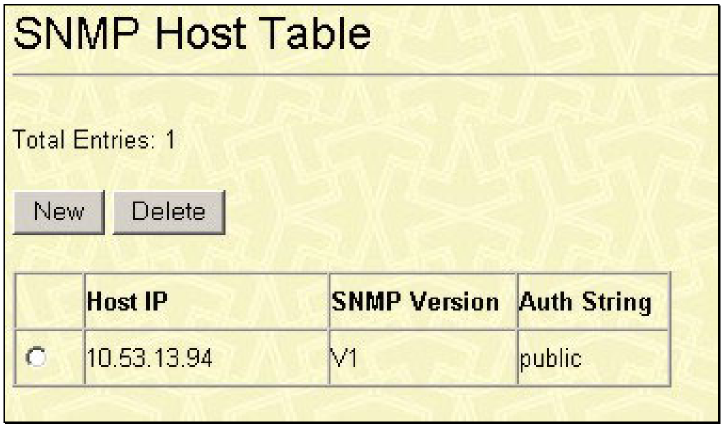
read_write – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch.

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.



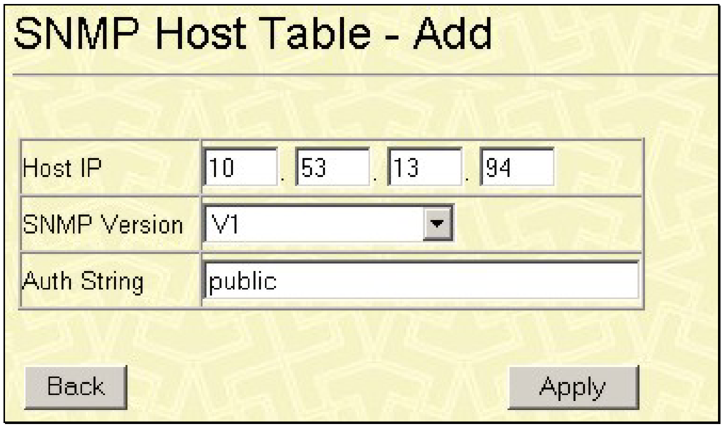
SNMP Host Table

Total Entries: 1

	Host IP	SNMP Version	Auth String
○	10.53.13.94	V1	public

Figure 5- 17. SNMP Host Table

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 Configuration** page, as shown below.



SNMP Host Table - Add

Host IP	10 . 53 . 13 . 94
SNMP Version	V1
Auth String	public

Figure 5- 18. SNMP Host Table – Add

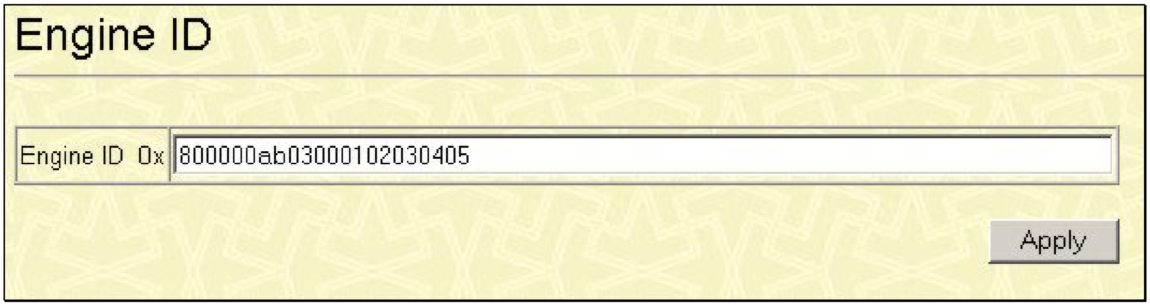
The following parameters can be set:

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.


Engine ID

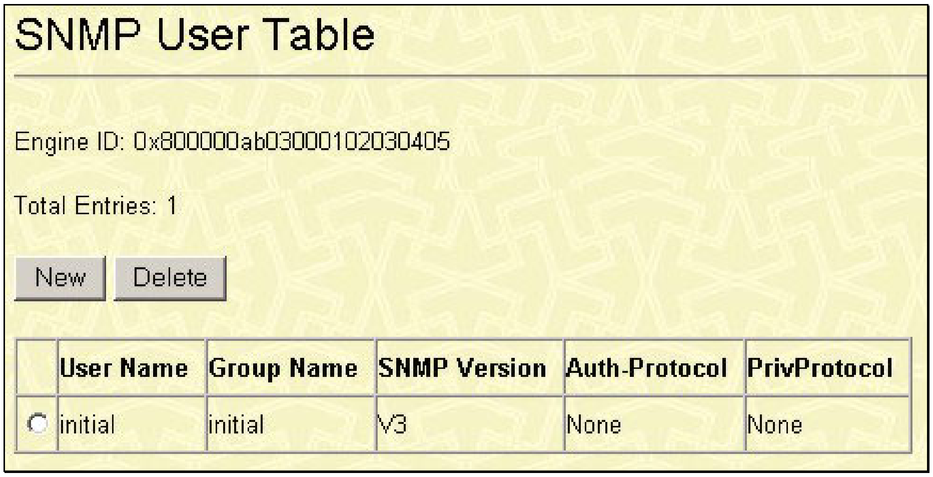
Engine ID 0x 800000ab03000102030405

Figure 5- 19. 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.



SNMP User Table

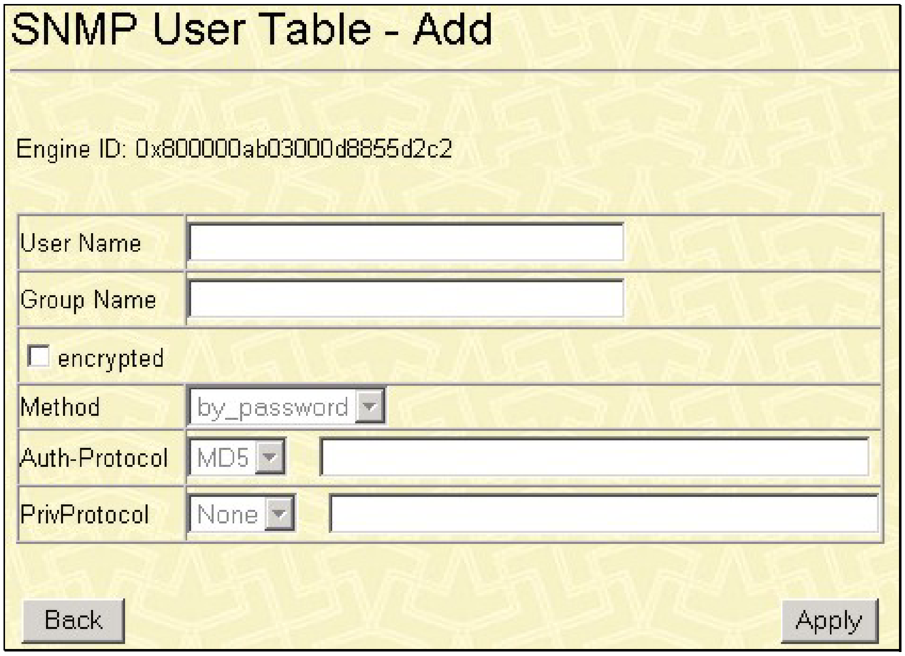
Engine ID: 0x800000ab03000102030405

Total Entries: 1

	User Name	Group Name	SNMP Version	Auth-Protocol	PrivProtocol
○	initial	initial	V3	None	None

Figure 5- 20. SNMP User Table

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.



SNMP User Table - Add

Engine ID: 0x800000ab03000d8855d2c2

User Name	
Group Name	
□ encrypted	
Method	by_password
Auth-Protocol	MD5
PrivProtocol	None

Figure 5- 21. SNMP User Table - Add

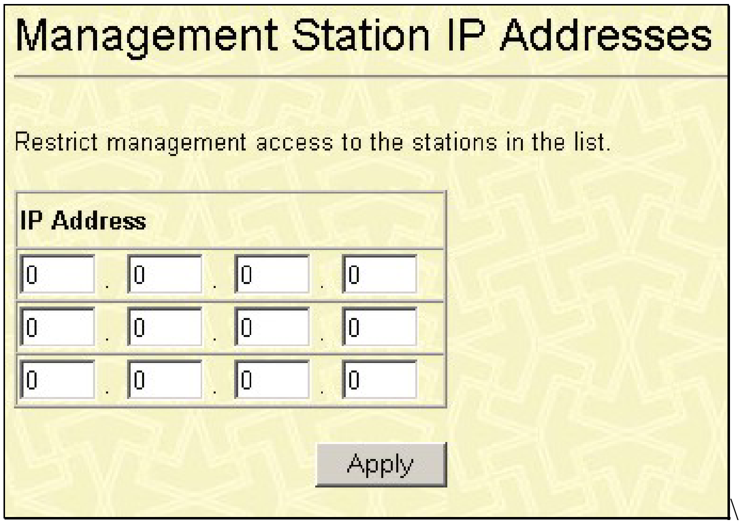
The following parameters can be set:

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.

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.

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.



Management Station IP Addresses

Restrict management access to the stations in the list.

IP Address
0 . 0 . 0 . 0
0 . 0 . 0 . 0
0 . 0 . 0 . 0

Figure 5- 22. Management Station IP Addresses window

Switch Utilities

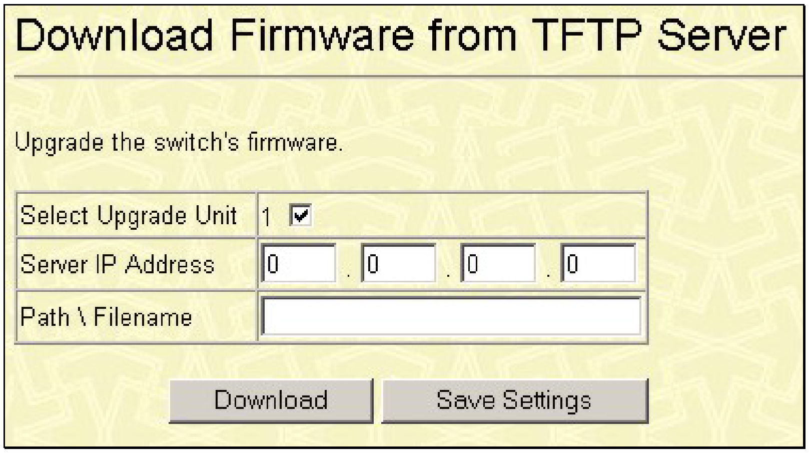
The **Switch Utilities** menu will aid the user in maintaining some of the basic utilities of the switch, such as TFTP services and the Ping test. See below for further description.

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

To update the Switch's firmware, click **Basic Setup** > **TFTP Services** > **Download Firmware from TFTP Server**:



Download Firmware from TFTP Server

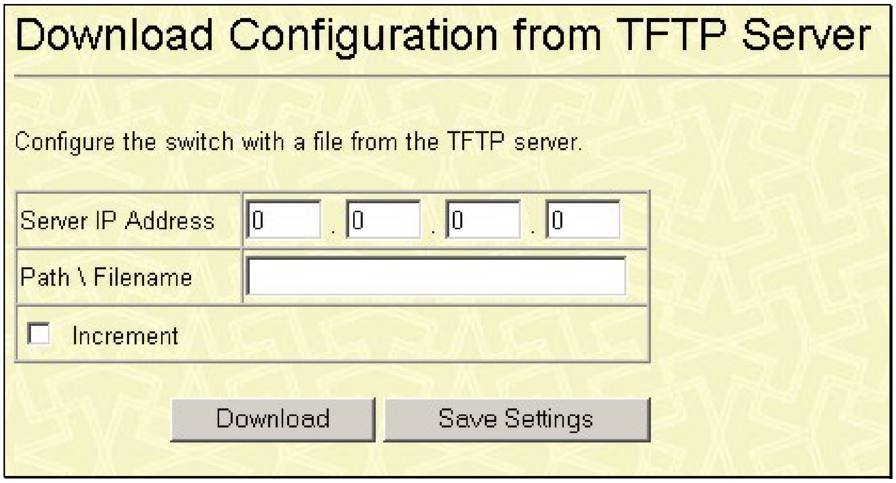
Upgrade the switch's firmware.

Select Upgrade Unit	1 ☑
Server IP Address	0 . 0 . 0 . 0
Path \ Filename	

Figure 5- 23. Download Firmware from TFTP Server window

Download Configuration File

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.



Download Configuration from TFTP Server

Configure the switch with a file from the TFTP server.

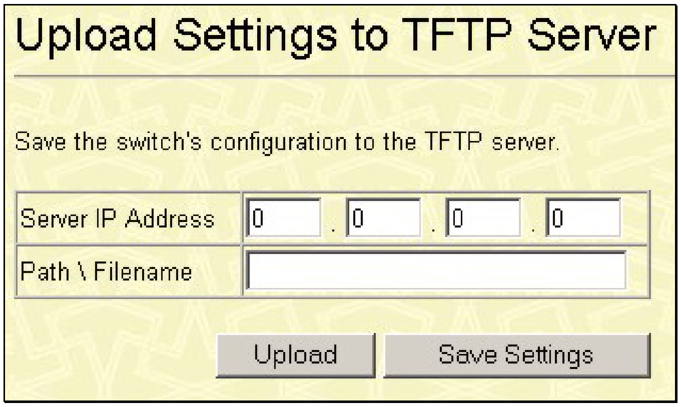
Server IP Address	0 . 0 . 0 . 0
Path \ Filename	
☐ Increment	

Figure 5- 24. Download Configuration from TFTP Server window

- Enter the IP address of the TFTP server and specify the location of the Switch configuration file on the TFTP server.
- Enter the full location of the firmware in the **Path/Filename** field.
- 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.
- Click **Save Settings** to record the IP address of the TFTP server.
- Click **Download** to initiate the file transfer.

Upload Settings to TFTP Server

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



Upload Settings to TFTP Server

Save the switch's configuration to the TFTP server.

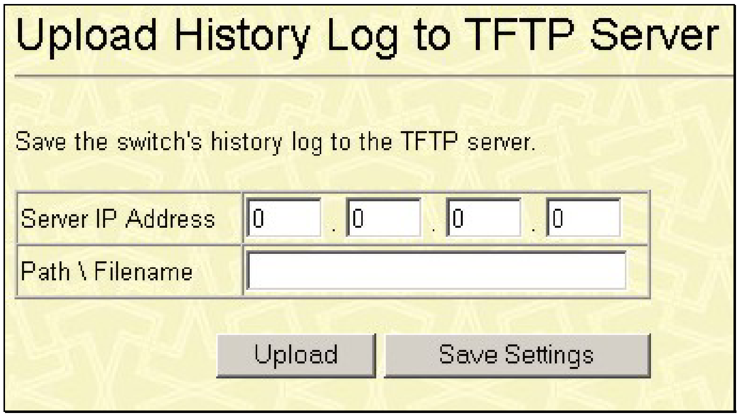
Server IP Address	0 . 0 . 0 . 0
Path \ Filename	

Figure 5- 25. Upload Settings to TFTP Server window

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

Save Switch History to TFTP Server

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:



Upload History Log to TFTP Server

Save the switch's history log to the TFTP server.

Server IP Address	0 . 0 . 0 . 0
Path \ Filename	

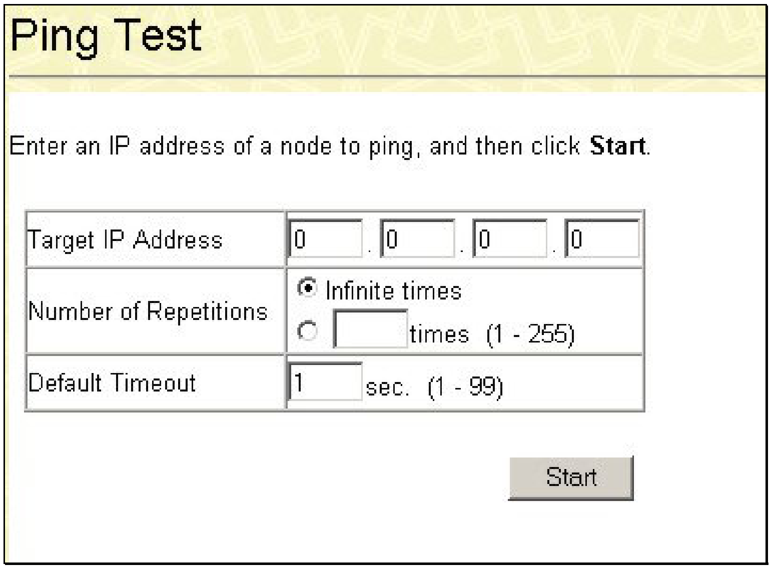
Figure 5- 26. Save Switch History to TFTP Server

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.

Click **Upload** to initiate the file transfer.

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.**



Ping Test

Enter an IP address of a node to ping, and then click **Start**.

Target IP Address	0 . 0 . 0 . 0
Number of Repetitions	● Infinite times ○ ____ times (1 - 255)
Default Timeout	1 sec. (1 - 99)

Figure 5- 27. 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.

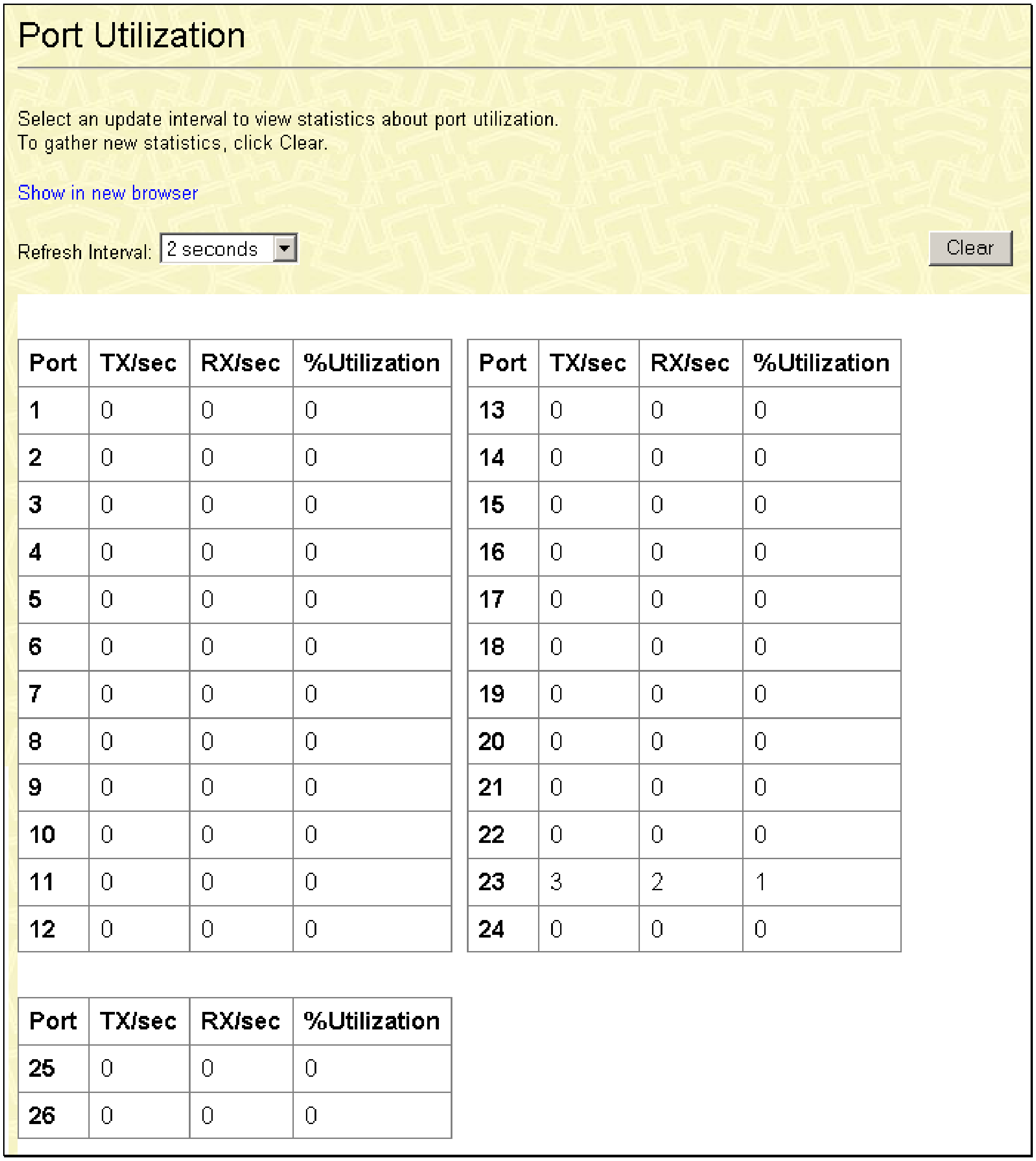
Network Monitoring

The DES-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.

Port Utilization

The **Port Utilization** page 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 Utilization

Select an update interval to view statistics about port utilization.
To gather new statistics, click Clear.

Refresh Interval: 2 seconds

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

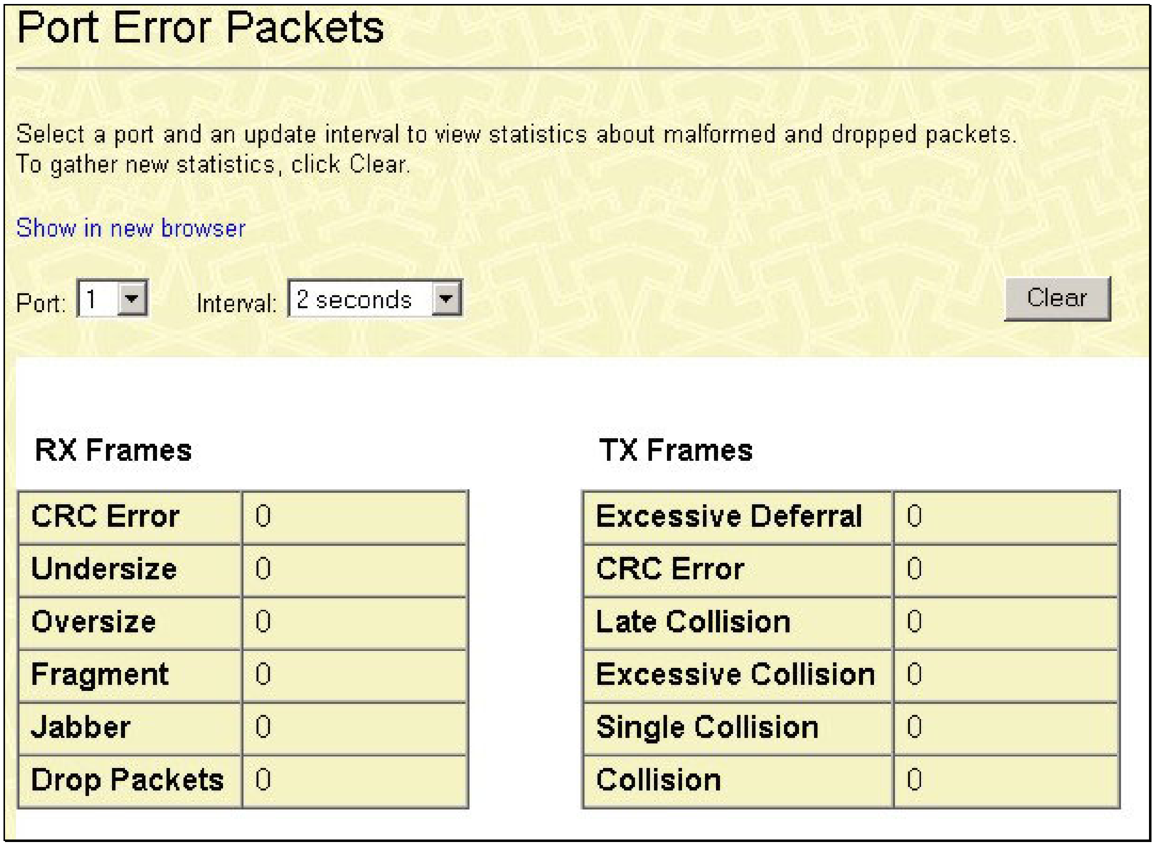
Port	TX/sec	RX/sec	%Utilization
25	0	0	0
26	0	0	0

Figure 5- 28. 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** screen, click **Basic Setup > Network Monitoring > Statistics > Port Error Packets**.



Port Error Packets

Select a port and an update interval to view statistics about malformed and dropped packets.
To gather new statistics, click Clear.

Show in new browser

Port: 1 Interval: 2 seconds

RX Frames

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

TX Frames

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

Figure 5- 29. Port Error Packets

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 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

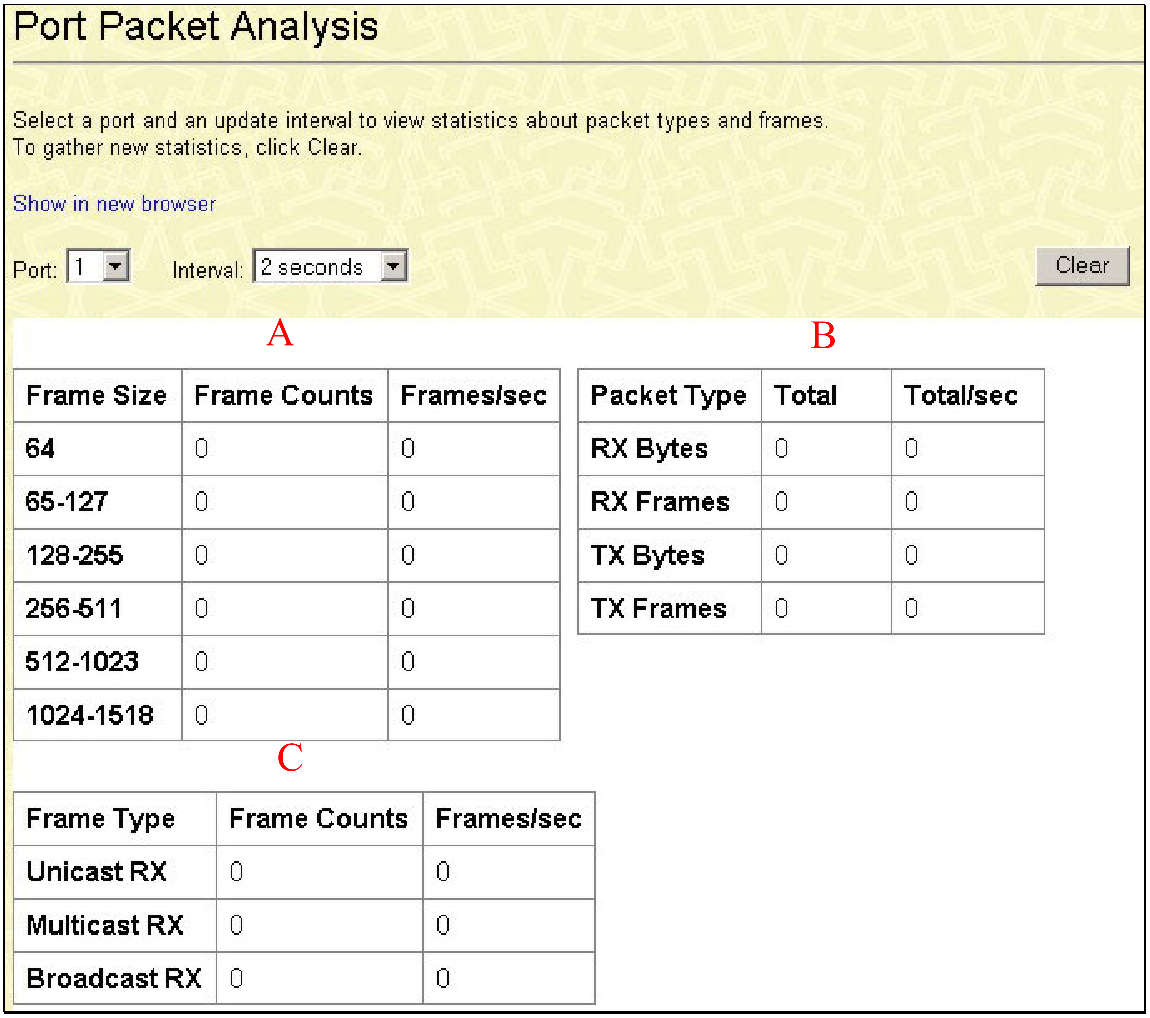
	frame 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	The number of frames with lengths more than the MAX_PKT_LEN bytes. 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.



Port Packet Analysis

Select a port and an update interval to view statistics about packet types and frames.
To gather new statistics, click Clear.

Show in new browser

Port: 1 Interval: 2 seconds Clear

Frame Size	Frame Counts	Frames/sec
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0

Packet Type	Total	Total/sec
RX Bytes	0	0
RX Frames	0	0
TX Bytes	0	0
TX Frames	0	0

Frame Type	Frame Counts	Frames/sec
Unicast RX	0	0
Multicast RX	0	0
Broadcast RX	0	0

Figure 5- 30. 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).
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**).

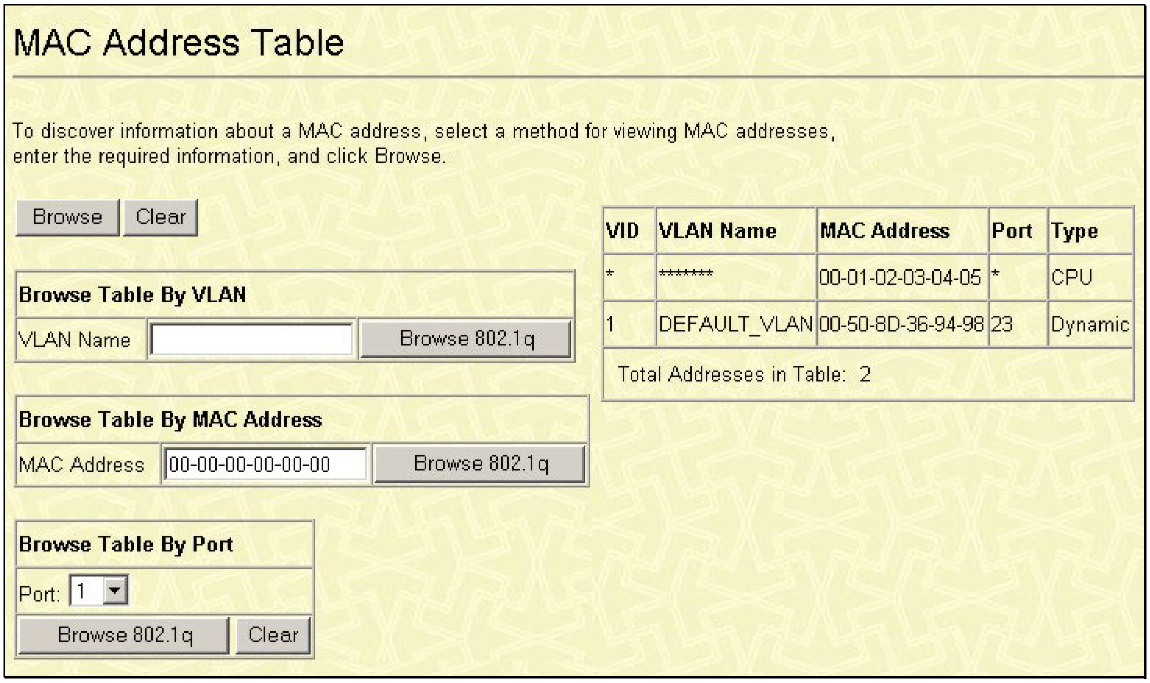
Table C: Frame Type

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**).

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**:



MAC Address Table

To discover information about a MAC address, select a method for viewing MAC addresses, enter the required information, and click Browse.

Browse Table By VLAN

VLAN Name

Browse Table By MAC Address

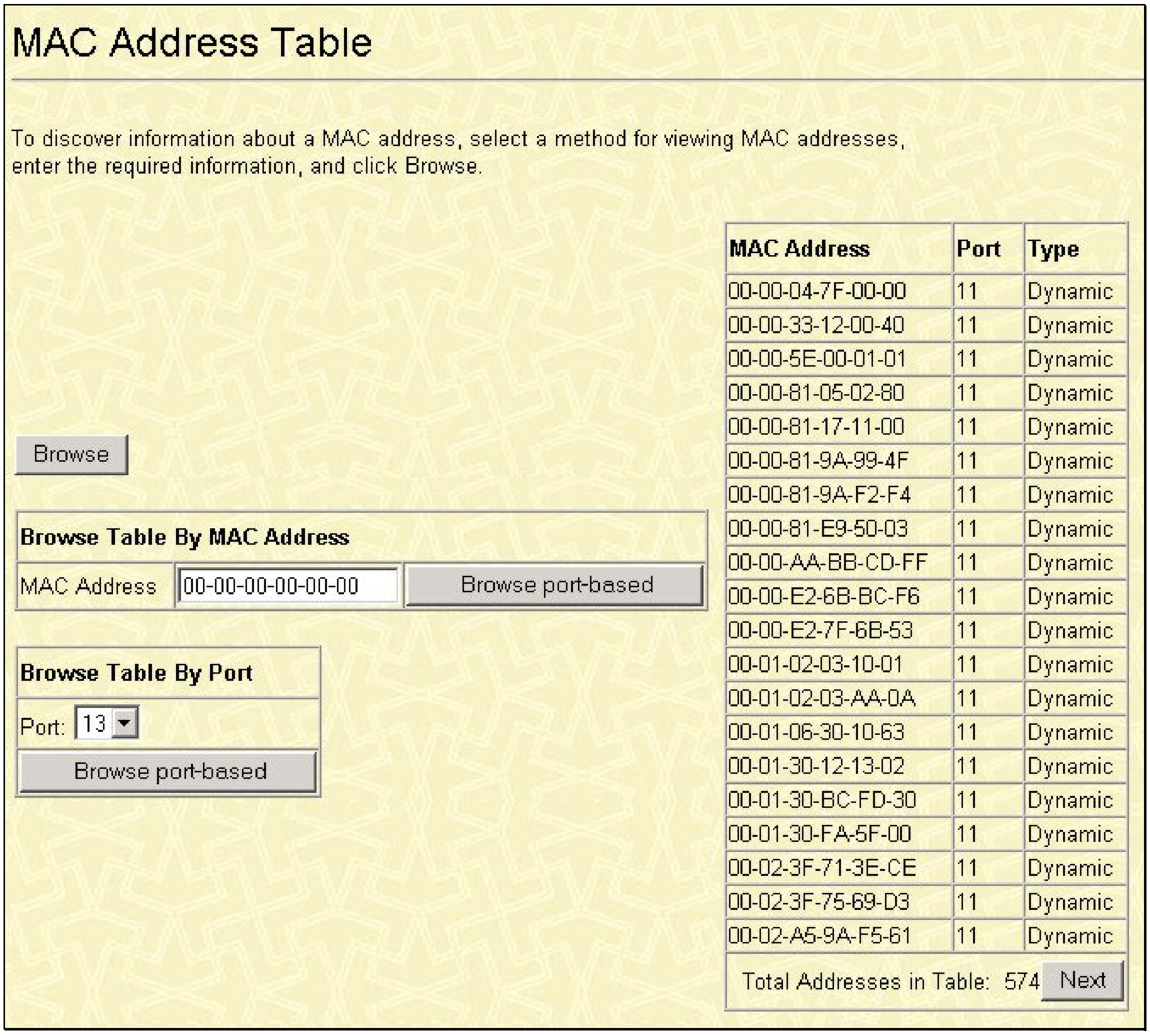
MAC Address 00-00-00-00-00-00

Browse Table By Port

Port: 1

VID	VLAN Name	MAC Address	Port	Type
*	*******	00-01-02-03-04-05	*	CPU
1	DEFAULT_VLAN	00-50-8D-36-94-98	23	Dynamic

Total Addresses in Table: 2



MAC Address Table

To discover information about a MAC address, select a method for viewing MAC addresses, enter the required information, and click Browse.

Browse Table By MAC Address

MAC Address: 00-00-00-00-00-00

Browse Table By Port

Port: 13

MAC Address	Port	Type
00-00-04-7F-00-00	11	Dynamic
00-00-33-12-00-40	11	Dynamic
00-00-5E-00-01-01	11	Dynamic
00-00-81-05-02-80	11	Dynamic
00-00-81-17-11-00	11	Dynamic
00-00-81-9A-99-4F	11	Dynamic
00-00-81-9A-F2-F4	11	Dynamic
00-00-81-E9-50-03	11	Dynamic
00-00-AA-BB-CD-FF	11	Dynamic
00-00-E2-6B-BC-F6	11	Dynamic
00-00-E2-7F-6B-53	11	Dynamic
00-01-02-03-10-01	11	Dynamic
00-01-02-03-AA-0A	11	Dynamic
00-01-06-30-10-63	11	Dynamic
00-01-30-12-13-02	11	Dynamic
00-01-30-BC-FD-30	11	Dynamic
00-01-30-FA-5F-00	11	Dynamic
00-02-3F-71-3E-CE	11	Dynamic
00-02-3F-75-69-D3	11	Dynamic
00-02-A5-9A-F5-61	11	Dynamic

Total Addresses in Table: 574

Figure 5- 31. Mac Address Table window

The following fields can be set:

Parameter	Description
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.
Next	Clicking this button forwards the table to the next screen of MAC Addresses.
Browse port-based.	Clicking this button will allow the user to browse the table by port-based MAC addresses.

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

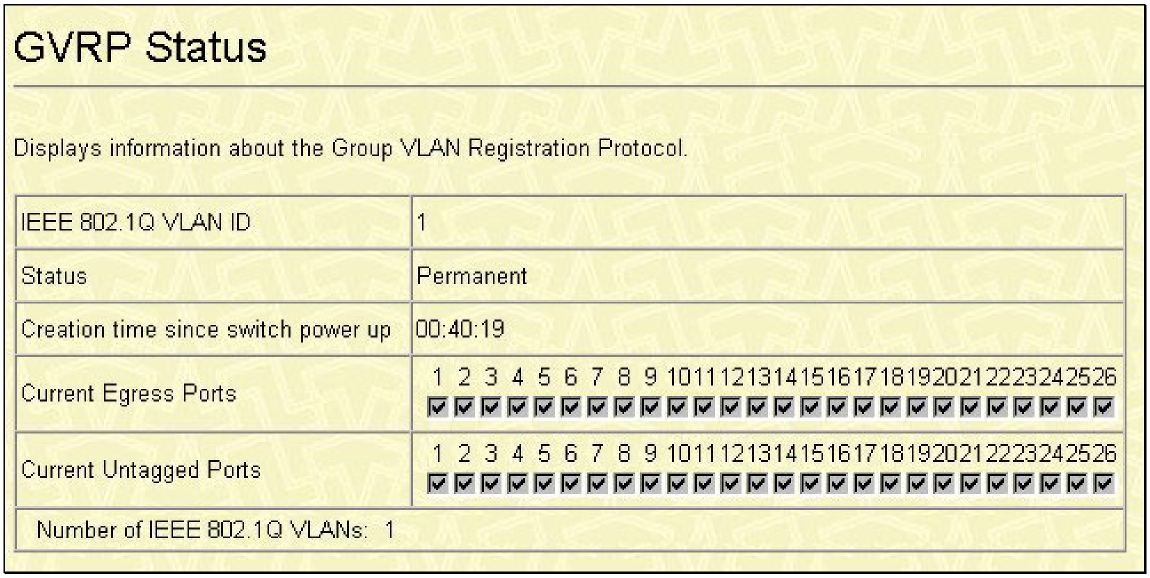
Parameter	Description
MAC Address	The MAC address entered into the address table.
Port	The port that the MAC address above corresponds to.
Type	How the switch discovered the MAC address. The possible entries are *Dynamic*, *Self*, and *Static*.

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.



GVRP Status

Displays information about the Group VLAN Registration Protocol.

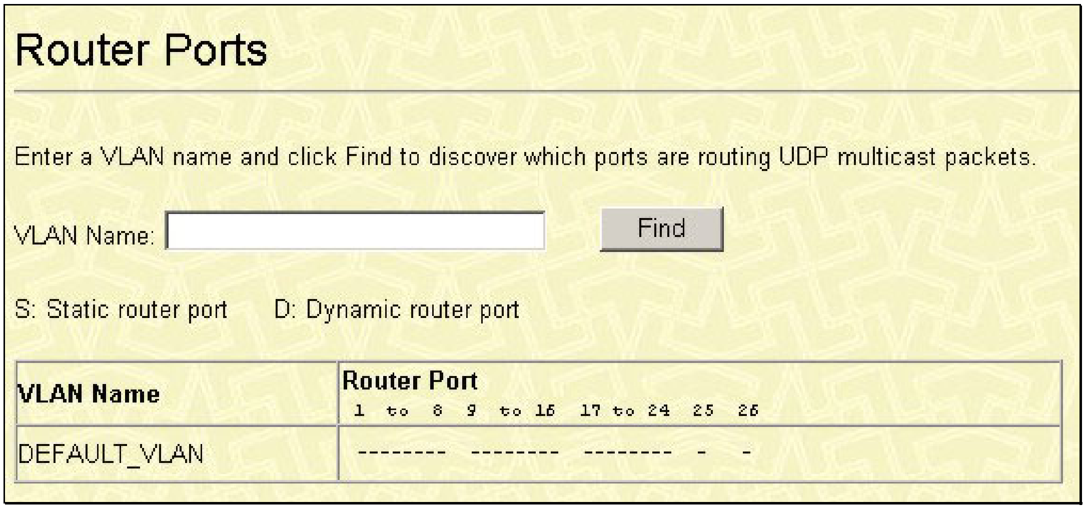
IEEE 802.1Q VLAN ID	1
Status	Permanent
Creation time since switch power up	00:40:19
Current Egress Ports	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ☑
Current Untagged Ports	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ☑
Number of IEEE 802.1Q VLANs: 1	

Figure 5- 32. 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**:



Router Ports

Enter a VLAN name and click Find to discover which ports are routing UDP multicast packets.

VLAN Name:

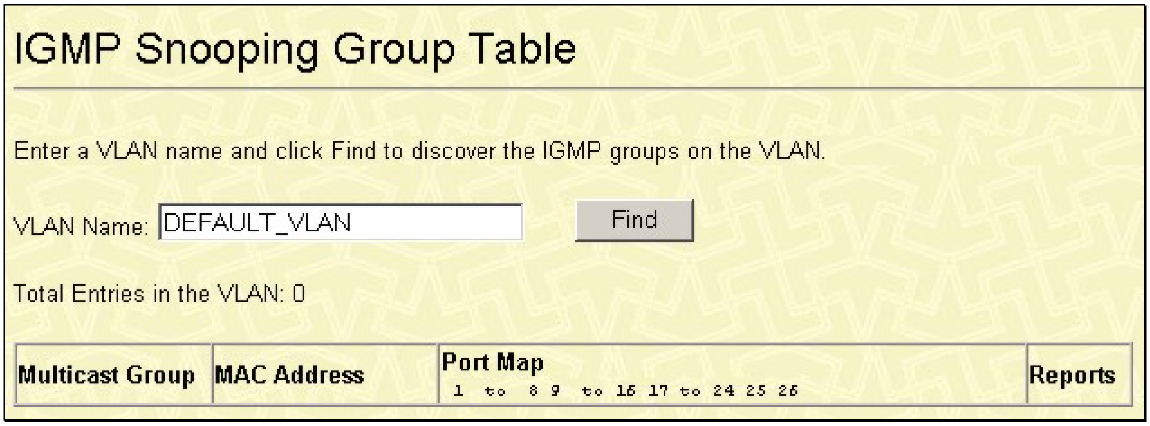
S: Static router port D: Dynamic router port

VLAN Name	Router Port 1 to 8 9 to 16 17 to 24 25 26
DEFAULT_VLAN	-------- -------- -------- - -

Figure 5- 33. Router Ports window

IGMP Snooping Group

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.



IGMP Snooping Group Table

Enter a VLAN name and click Find to discover the IGMP groups on the VLAN.

VLAN Name: DEFAULT_VLAN

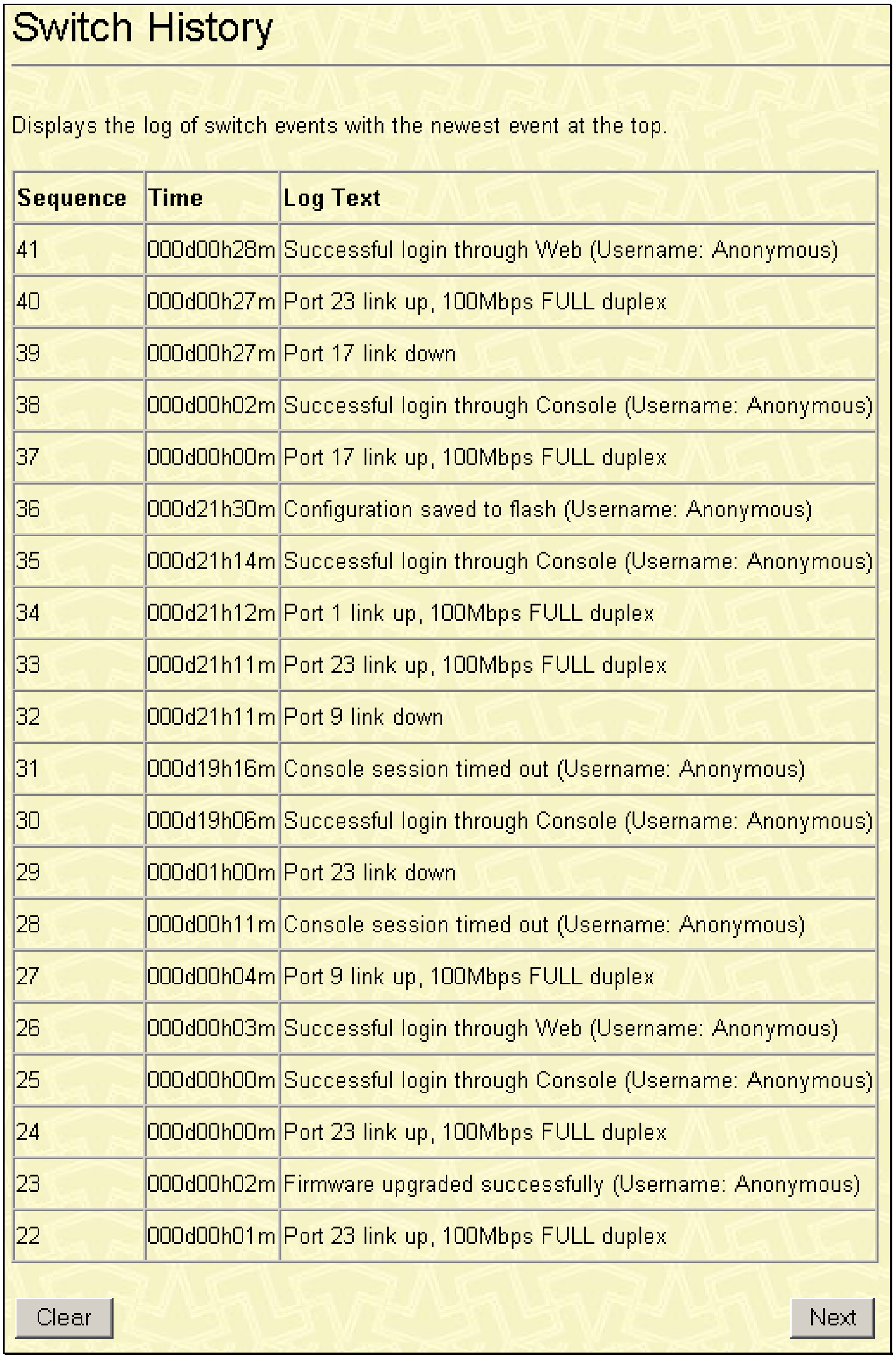
Total Entries in the VLAN: 0

Multicast Group	MAC Address	Port Map 1 to 8 9 to 16 17 to 24 25 26	Reports

Figure 5- 34. 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.



Switch History

Displays the log of switch events with the newest event at the top.

Sequence	Time	Log Text
41	000d00h28m	Successful login through Web (Username: Anonymous)
40	000d00h27m	Port 23 link up, 100Mbps FULL duplex
39	000d00h27m	Port 17 link down
38	000d00h02m	Successful login through Console (Username: Anonymous)
37	000d00h00m	Port 17 link up, 100Mbps FULL duplex
36	000d21h30m	Configuration saved to flash (Username: Anonymous)
35	000d21h14m	Successful login through Console (Username: Anonymous)
34	000d21h12m	Port 1 link up, 100Mbps FULL duplex
33	000d21h11m	Port 23 link up, 100Mbps FULL duplex
32	000d21h11m	Port 9 link down
31	000d19h16m	Console session timed out (Username: Anonymous)
30	000d19h06m	Successful login through Console (Username: Anonymous)
29	000d01h00m	Port 23 link down
28	000d00h11m	Console session timed out (Username: Anonymous)
27	000d00h04m	Port 9 link up, 100Mbps FULL duplex
26	000d00h03m	Successful login through Web (Username: Anonymous)
25	000d00h00m	Successful login through Console (Username: Anonymous)
24	000d00h00m	Port 23 link up, 100Mbps FULL duplex
23	000d00h02m	Firmware upgraded successfully (Username: Anonymous)
22	000d00h01m	Port 23 link up, 100Mbps FULL duplex

Figure 5- 35. Switch History window

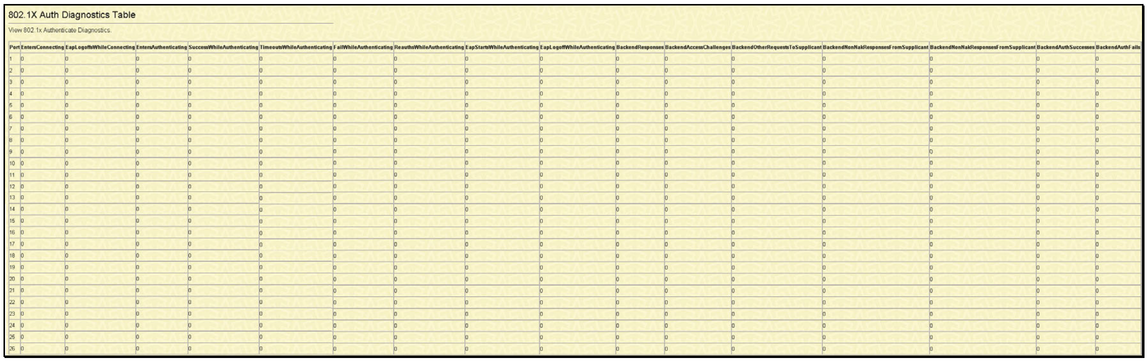
The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Clicking **Next** at the bottom of the window will allow you to display all the switch Trap Logs.

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.

802.1X Auth Diagnostics Table

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



802.1X Auth Diagnostics Table

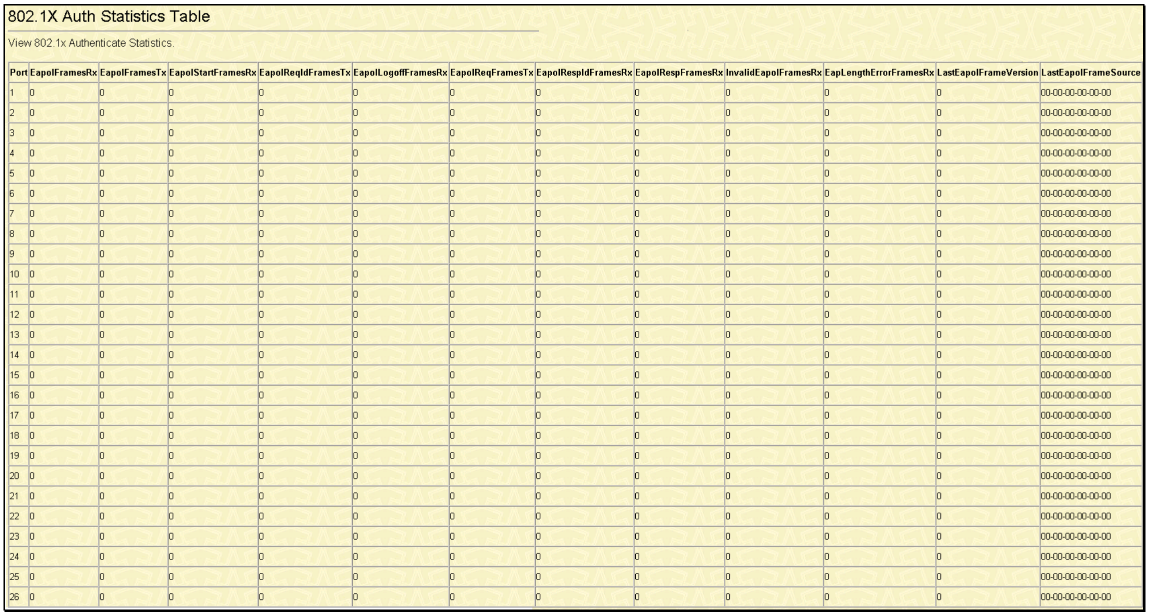
View 802.1x Authenticate Diagnostics.

Port	EntersConnecting	EapLogoffsWhileConnecting	EntersAuthenticating	SuccessWhileAuthenticating	TimeoutsWhileAuthenticating	FailWhileAuthenticating	ReauthsWhileAuthenticating	EapStartsWhileAuthenticating	EapLogoffWhileAuthenticating	BackendResponses	BackendAccessChallenges	BackendOtherRequestsToSupplicant	BackendNonNakResponsesFromSupplicant	BackendNonNakResponsesFromSupplicant	BackendAuthSuccesses	BackendAuthFails
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 5- 36. 802.1X Auth Diagnostics Table

802.1X Auth Statistics Table

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

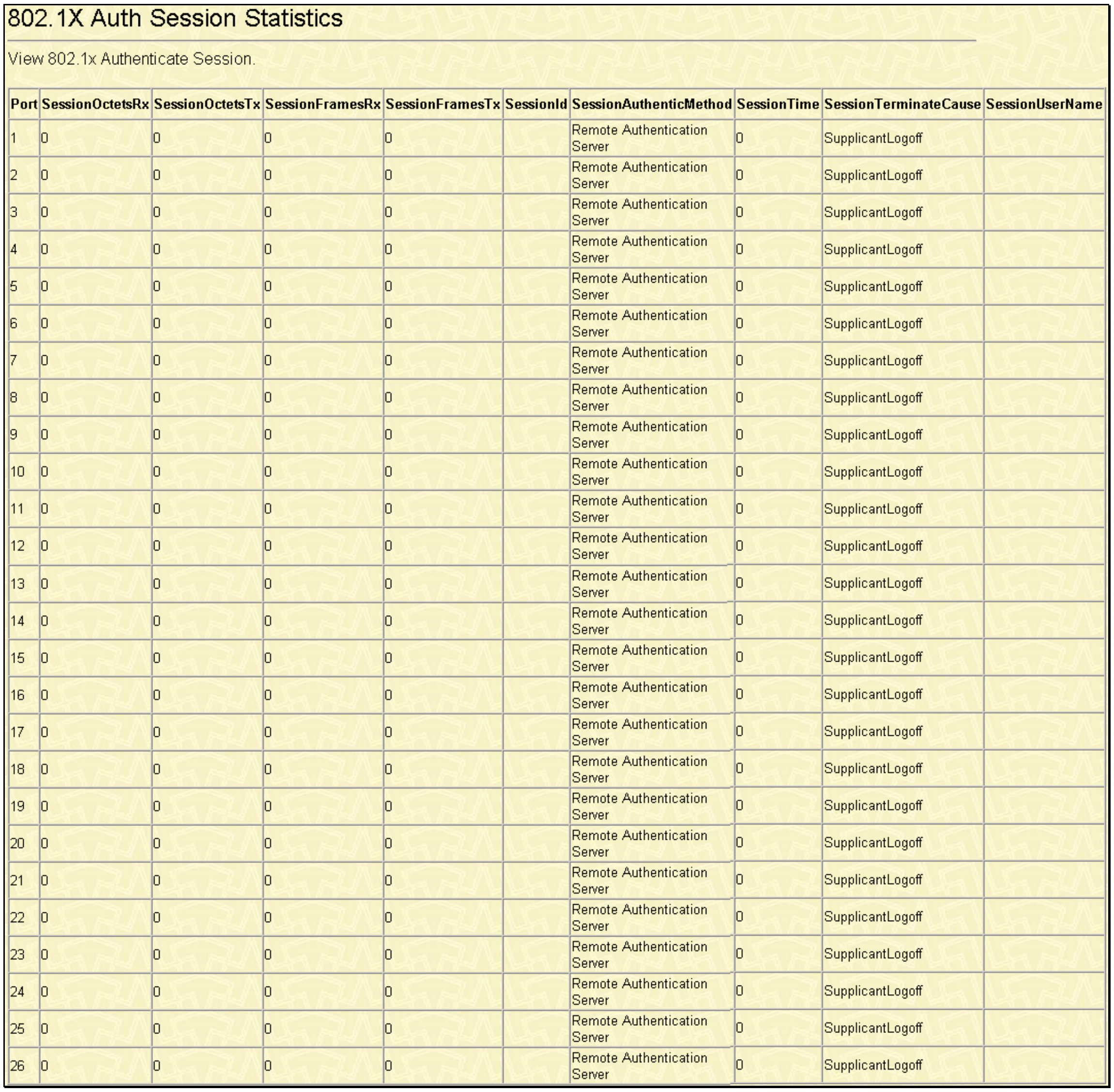
View 802.1x Authenticate Statistics.

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 5- 37. 802.1X Auth Statistics Table

802.1X Auth Session 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 Session.**



802.1X Auth Session Statistics

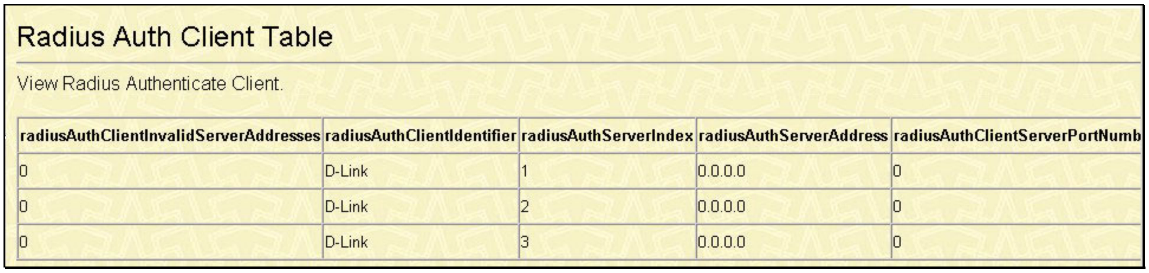
View 802.1x Authenticate Session.

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 5- 38. 802.1X Auth Session Statistics window

RADIUS Auth Client Table

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

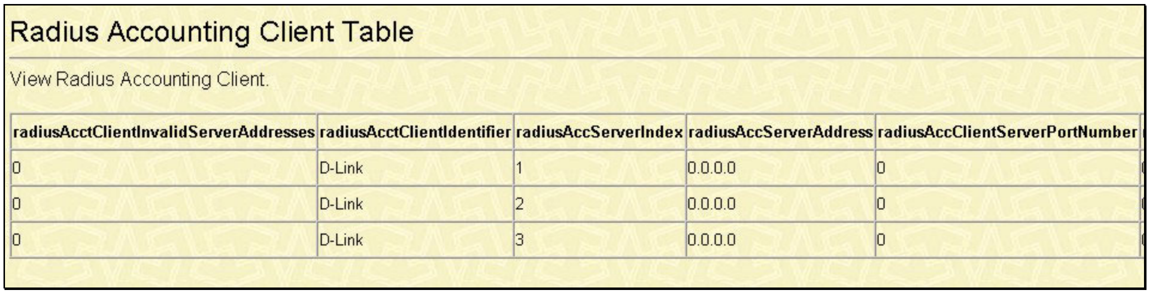
View Radius Authenticate Client.

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 5- 39. RADIUS Auth Client Table

RADIUS Accounting Table

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 Accounting Client Table

View Radius Accounting Client.

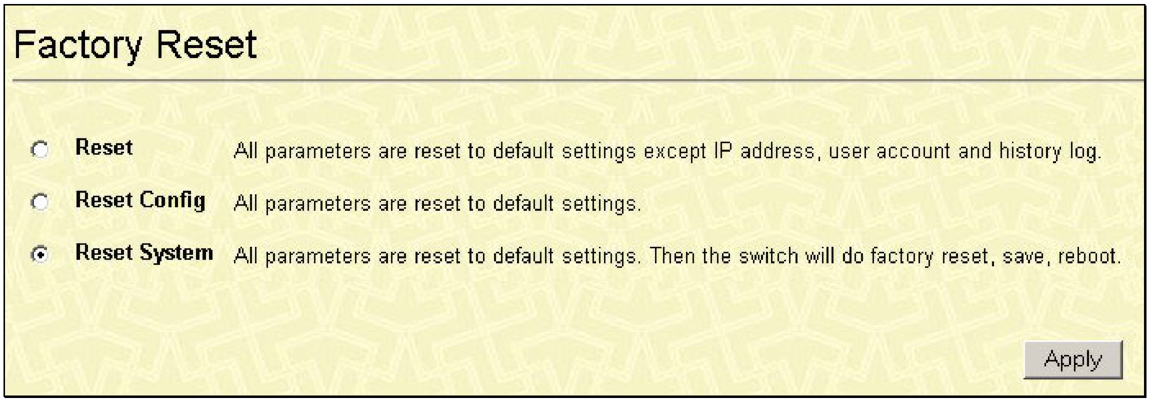
radiusAcctClientInvalidServerAddresses	radiusAcctClientIdentifier	radiusAccServerIndex	radiusAccServerAddress	radiusAccClientServerPortNumber
0	D-Link	1	0.0.0.0	0
0	D-Link	2	0.0.0.0	0
0	D-Link	3	0.0.0.0	0

Figure 5- 40. RADIUS Accounting Table

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.



Factory Reset

○ **Reset** All parameters are reset to default settings except IP address, user account and history log.

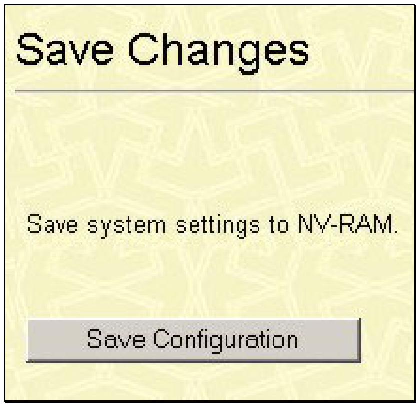
○ **Reset Config** All parameters are reset to default settings.

● **Reset System** All parameters are reset to default settings. Then the switch will do factory reset, save, reboot.

Figure 5- 41. Factory Reset window

Save Changes

The DES-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.

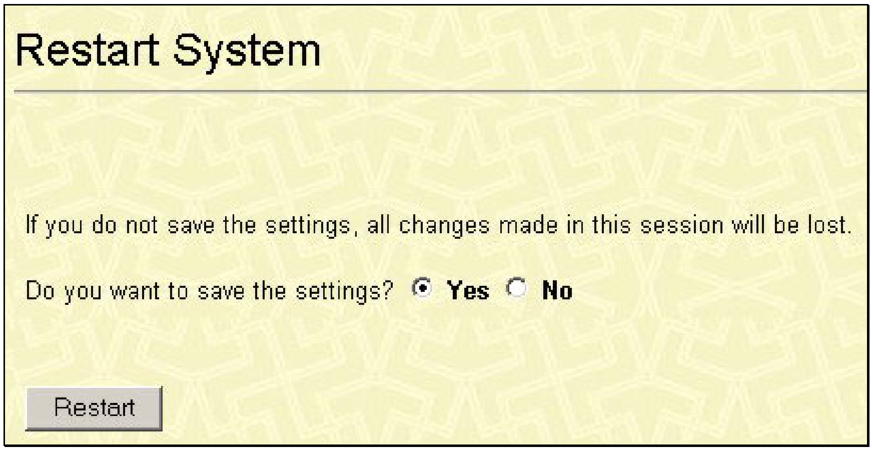


Save Changes

Save system settings to NV-RAM.

Figure 5- 42. Save Changes window

Restart System



Restart System

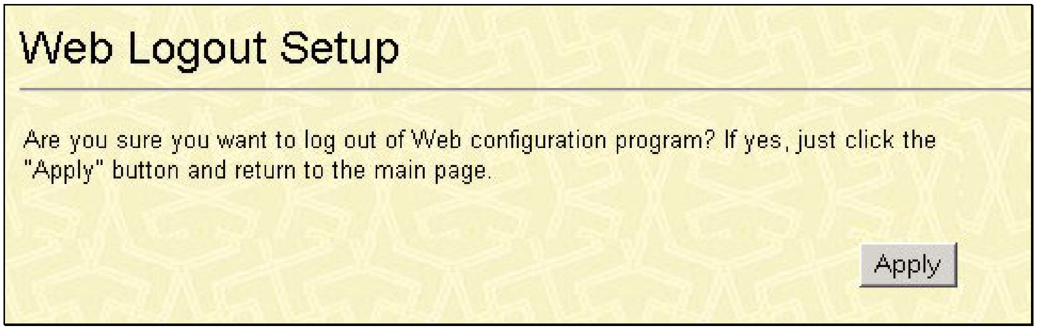
If you do not save the settings, all changes made in this session will be lost.

Do you want to save the settings? ● Yes ○ No

Figure 5- 43. Restart System window

Logout

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



Web Logout Setup

Are you sure you want to log out of Web configuration program? If yes, just click the "Apply" button and return to the main page.

Figure 5- 44. Web Logout Setup window.

To logout of the Web configuration, simply click Apply.

Section 6

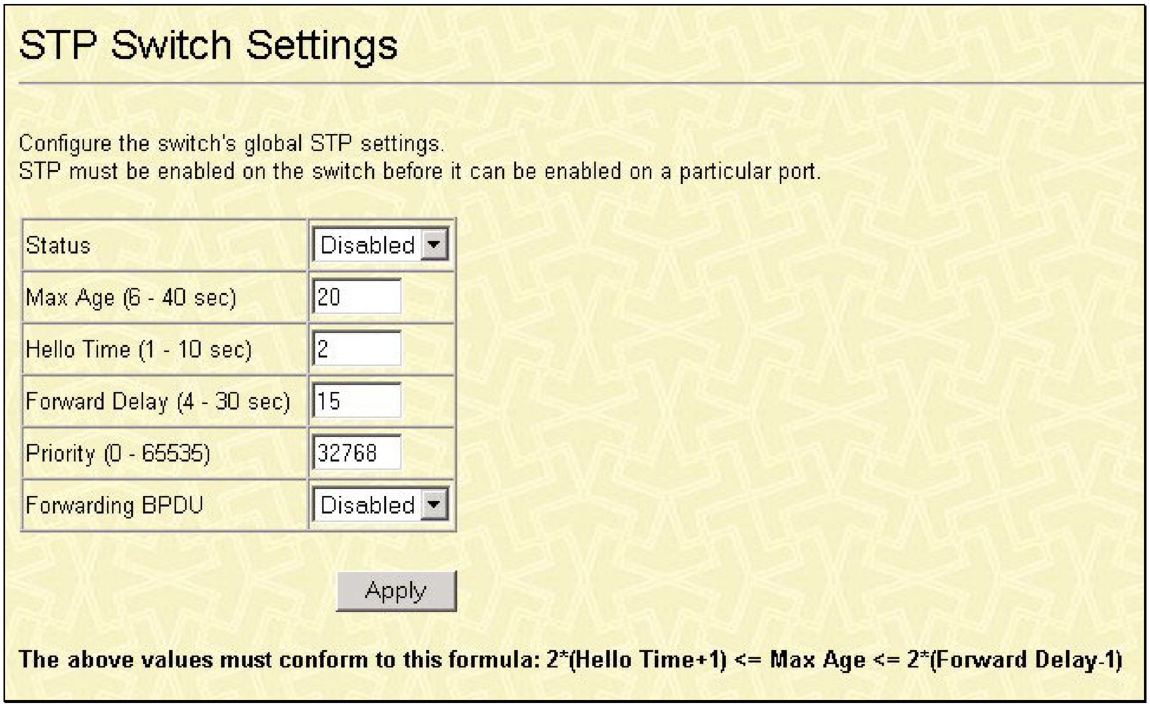
Advanced Setup

Configuring The 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:

STP Switch Settings

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



STP Switch Settings

Configure the switch's global STP settings.
STP must be enabled on the switch before it can be enabled on a particular port.

Status	Disabled
Max Age (6 - 40 sec)	20
Hello Time (1 - 10 sec)	2
Forward Delay (4 - 30 sec)	15
Priority (0 - 65535)	32768
Forwarding BPDU	Disabled

The above values must conform to this formula: 2*(Hello Time+1) <= Max Age <= 2*(Forward Delay-1)

Figure 6- 1. 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 (0-65535)	<*32768*> – A Bridge Priority can be from 0 to 65535. Zero is equal to the highest Bridge Priority.
Forwarding BPDU (Disabled)	This can 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)

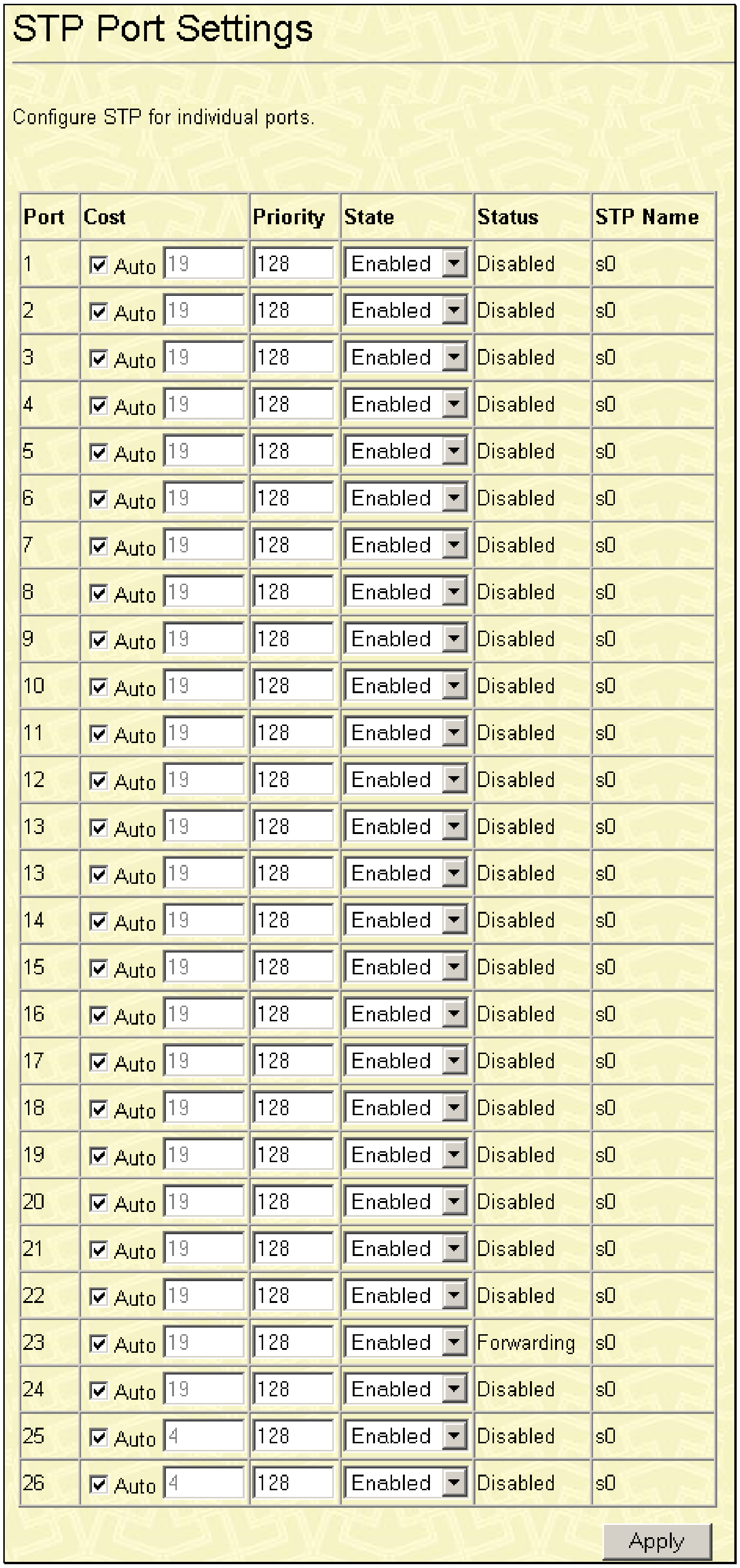
Note: The Spanning Tree Protocol (STP) operates on two levels: On the switch level, the settings are globally implemented. On the port level, the settings are implemented on a per user-defined Group basis.

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.

STP Port Settings

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



STP Port Settings

Configure STP for individual ports.

Port	Cost	Priority	State	Status	STP Name
1	☑ Auto 19	128	Enabled	Disabled	s0
2	☑ Auto 19	128	Enabled	Disabled	s0
3	☑ Auto 19	128	Enabled	Disabled	s0
4	☑ Auto 19	128	Enabled	Disabled	s0
5	☑ Auto 19	128	Enabled	Disabled	s0
6	☑ Auto 19	128	Enabled	Disabled	s0
7	☑ Auto 19	128	Enabled	Disabled	s0
8	☑ Auto 19	128	Enabled	Disabled	s0
9	☑ Auto 19	128	Enabled	Disabled	s0
10	☑ Auto 19	128	Enabled	Disabled	s0
11	☑ Auto 19	128	Enabled	Disabled	s0
12	☑ Auto 19	128	Enabled	Disabled	s0
13	☑ Auto 19	128	Enabled	Disabled	s0
13	☑ Auto 19	128	Enabled	Disabled	s0
14	☑ Auto 19	128	Enabled	Disabled	s0
15	☑ Auto 19	128	Enabled	Disabled	s0
16	☑ Auto 19	128	Enabled	Disabled	s0
17	☑ Auto 19	128	Enabled	Disabled	s0
18	☑ Auto 19	128	Enabled	Disabled	s0
19	☑ Auto 19	128	Enabled	Disabled	s0
20	☑ Auto 19	128	Enabled	Disabled	s0
21	☑ Auto 19	128	Enabled	Disabled	s0
22	☑ Auto 19	128	Enabled	Disabled	s0
23	☑ Auto 19	128	Enabled	Forwarding	s0
24	☑ Auto 19	128	Enabled	Disabled	s0
25	☑ Auto 4	128	Enabled	Disabled	s0
26	☑ Auto 4	128	Enabled	Disabled	s0

Figure 6- 2. STP Port Settings window

The STP port settings that can be configured or viewed are:

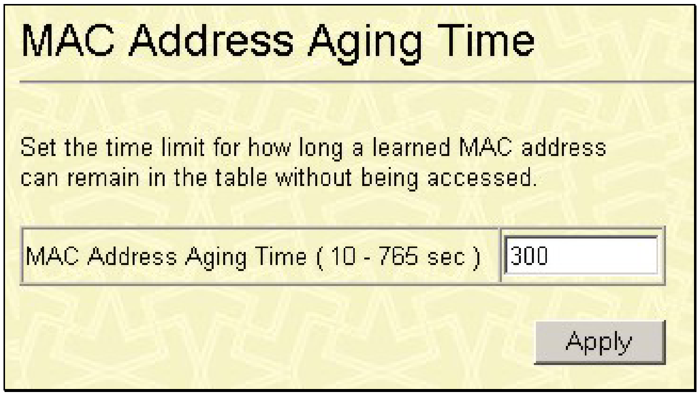
Parameter	Description
Port	Port number.
Cost	A Port Cost can be set from *1* to *65535*. The lower the number, the greater the probability the port will be chosen to forward packets.
Priority	A Port Priority can be from *0* to *255*. The lower the number, the greater the probability the port will be chosen as the Root Port.
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.
Status	Current status of the individual ports, whether it be *enabled* or *disabled*.
STP Name	Name of the STP associated with the corresponding 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**.

Configuring MAC Forwarding

MAC Forwarding

MAC Address Aging Time



MAC Address Aging Time

Set the time limit for how long a learned MAC address can remain in the table without being accessed.

MAC Address Aging Time (10 - 765 sec)	300

Figure 6- 3. MAC Address Aging Time window

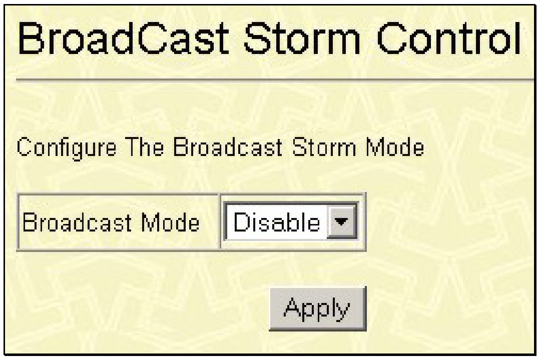
The information on the window is described as follows:

MAC Address Aging Time (10 – 765 sec)] <*300* > **–** This 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.

Broadcast Storm Control

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.



BroadCast Storm Control

Configure The Broadcast Storm Mode

Broadcast Mode: Disable

Figure 6- 4. Broadcast Storm Control window

Configuring QoS

The DES-3226L supports 802.1p priority queuing. The switch has two priority queues. These priority queues are labeled as 1, the high queue, and 0, 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 8 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.

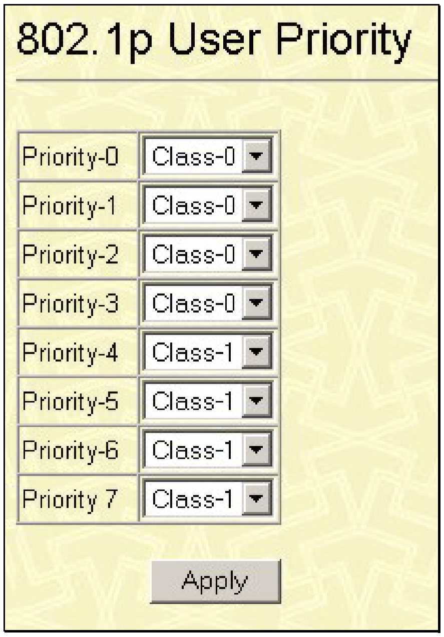
For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

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

802.1p User Priority

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



802.1p User Priority

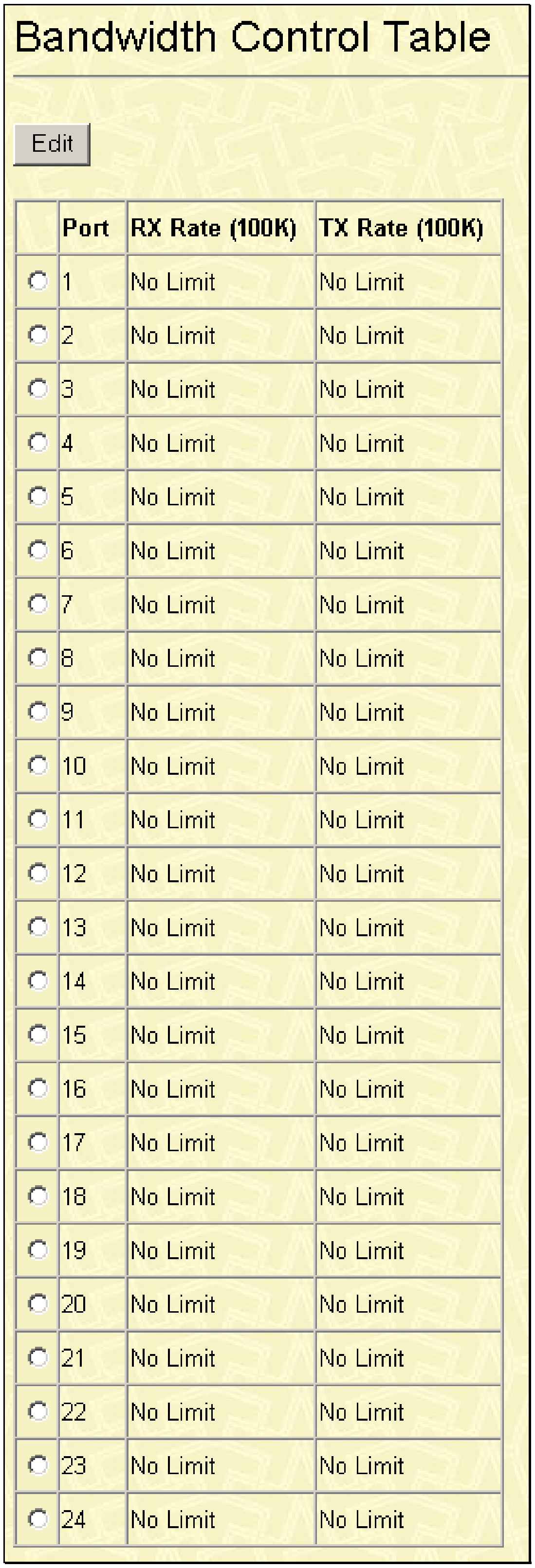
Priority-0	Class-0
Priority-1	Class-0
Priority-2	Class-0
Priority-3	Class-0
Priority-4	Class-1
Priority-5	Class-1
Priority-6	Class-1
Priority 7	Class-1

Figure 6- 5. 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 8 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.

Bandwidth Control Table



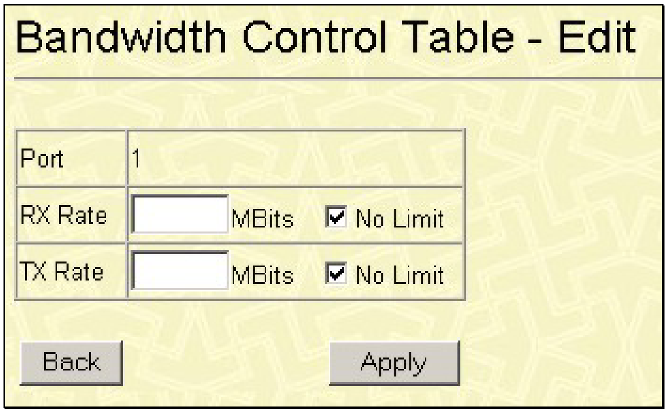
Bandwidth Control Table

	Port	RX Rate (100K)	TX Rate (100K)
○	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	No Limit

Figure 6- 6. 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:



Bandwidth Control Table - Edit

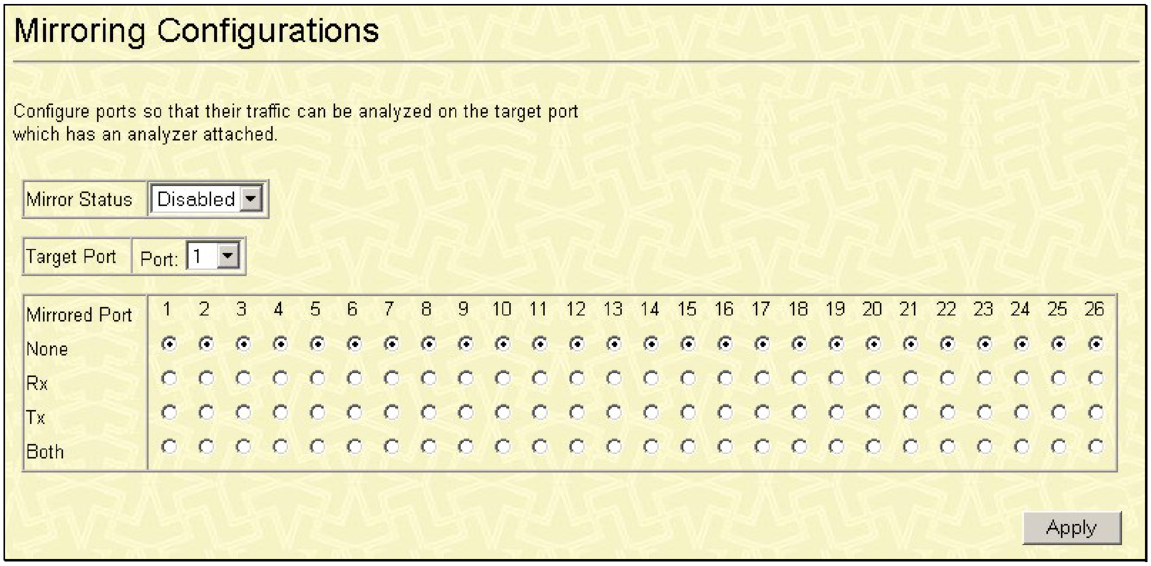
Port	1		
RX Rate		MBits	☑ No Limit
TX Rate		MBits	☑ No Limit

Figure 6- 7. 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.

Configuring Mirroring

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**.



Mirroring Configurations

Configure ports so that their traffic can be analyzed on the target port which has an analyzer attached.

Mirror Status: Disabled

Target Port: Port: 1

Mirrored Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Rx	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tx	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Both	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 6- 8. 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:

Parameter	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.

Configuring VLANs

Understanding IEEE 802.1p Priority

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 DES-3226L

1. 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.
2. The DES-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.
3. The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
4. The "default" has a VID = 1.
5. 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.

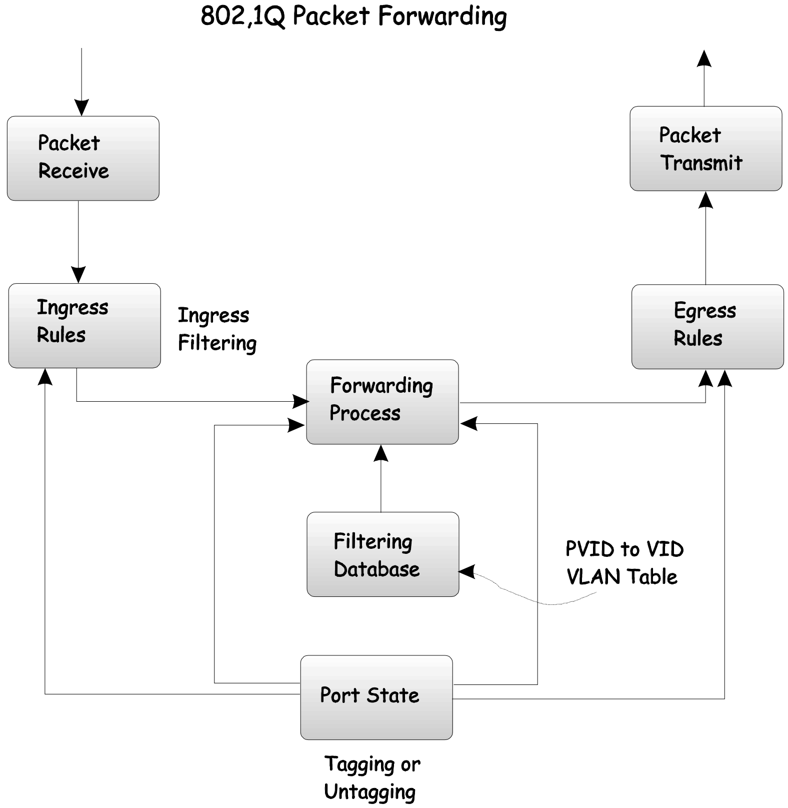


Figure 6- 9. IEEE 802.1Q Packet Forwarding

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.

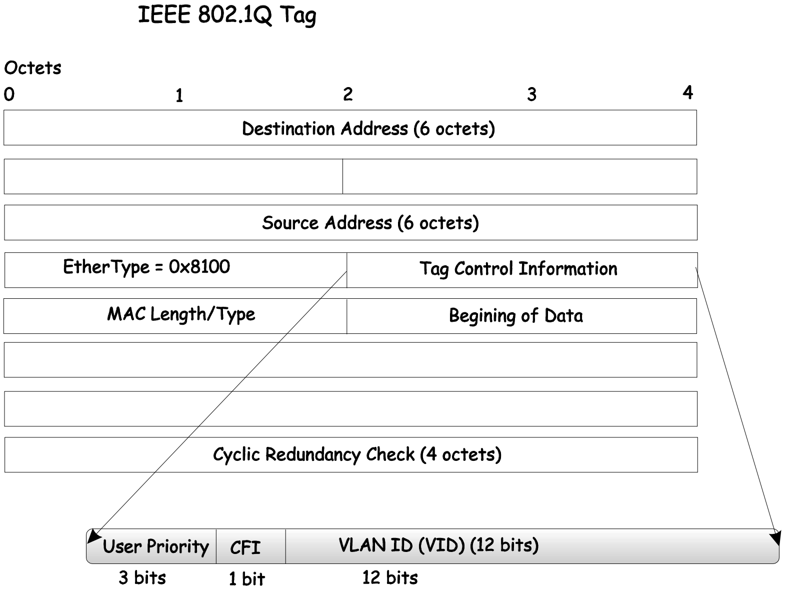


Figure 6- 10. IEEE 802.1Q Tag

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.

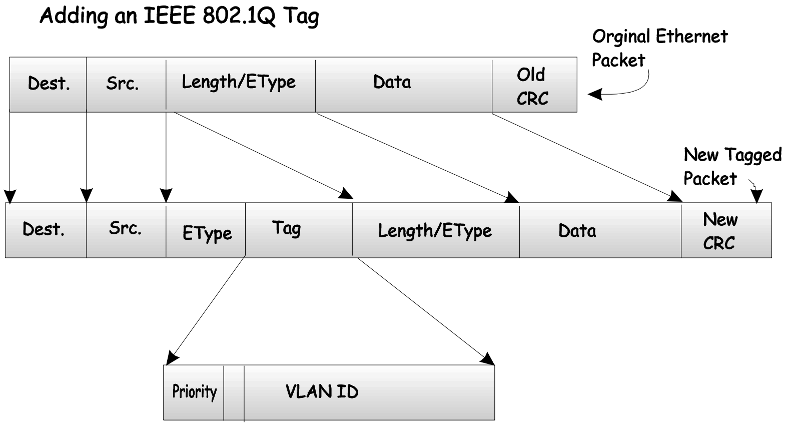


Figure 6- 11. Adding an IEEE 802.1Q Tag

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.

VLANs

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

Table 6- 1. VLAN Example – Assigned Ports

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.

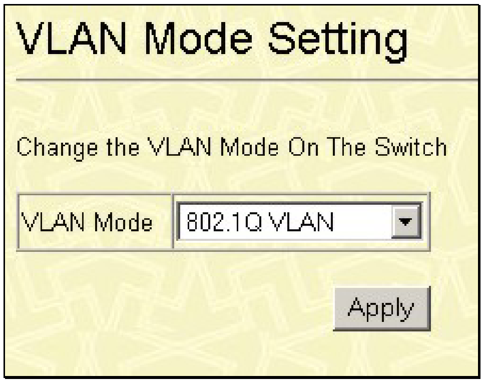
Network resources such as printers and servers however, can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, setting VLAN 1 members to ports 1, 2, 3, and 4 and VLAN 2 members to ports 1, 5, 6, and 7. Port 1 belongs 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.

VLAN Mode Set



VLAN Mode Setting

Change the VLAN Mode On The Switch

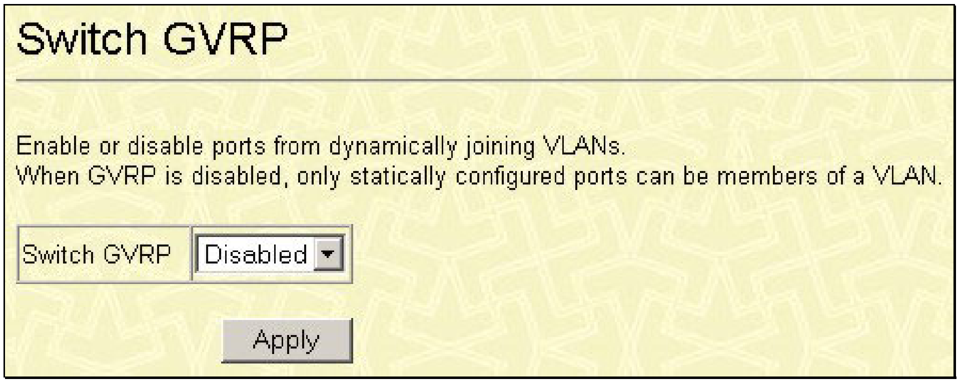
VLAN Mode: 802.1Q VLAN

Figure 6- 12. 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.

802.1Q VLANs

Switch GVRP



Switch GVRP

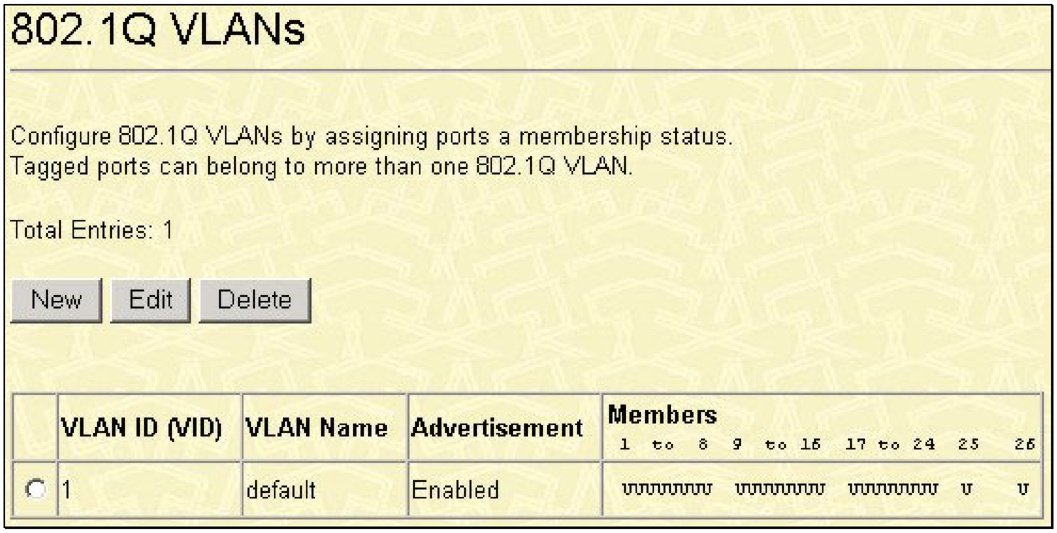
Enable or disable ports from dynamically joining VLANs.
When GVRP is disabled, only statically configured ports can be members of a VLAN.

Switch GVRP: Disabled

Figure 6- 13. Switch GVRP

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

802.1Q VLANs



802.1Q VLANs

Configure 802.1Q VLANs by assigning ports a membership status.
Tagged ports can belong to more than one 802.1Q VLAN.

Total Entries: 1

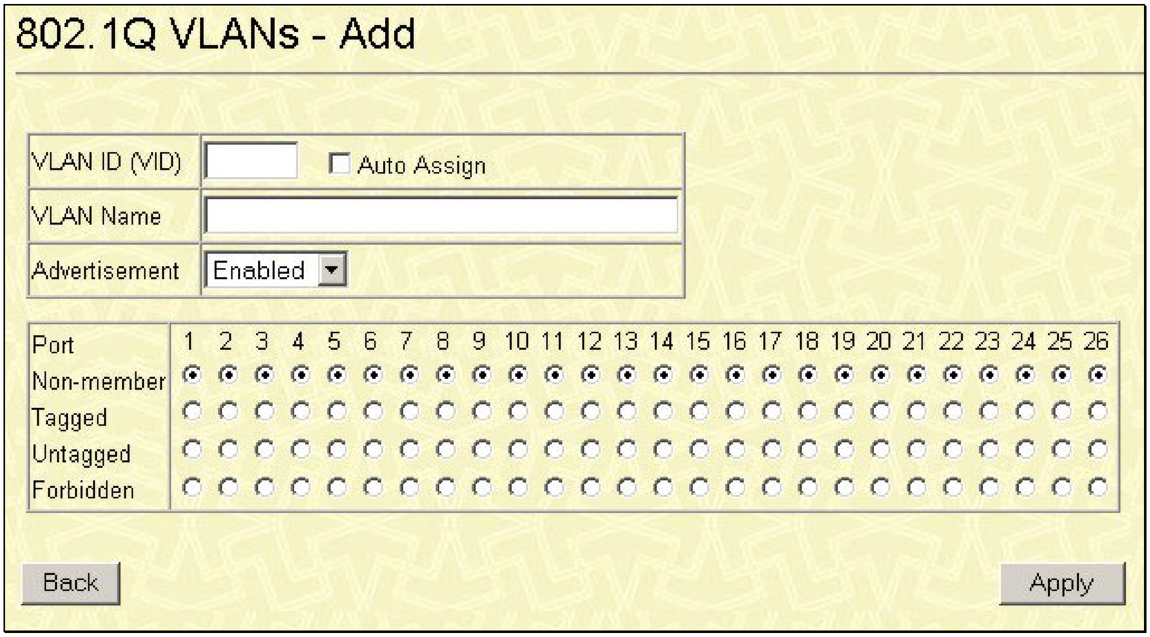
	VLAN ID (VID)	VLAN Name	Advertisement	Members 1 to 8 9 to 16 17 to 24 25 26
○	1	default	Enabled	uuuuuuuu uuuuuuuu uuuuuuuu u u

Figure 6- 14. 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	The VLAN ID of the VLAN that was created.
VLAN Name	The name of the VLAN that is being created.
Advertisement	Enabling this function will allow the switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port Members	Corresponds to the ports that are members of the particular VLAN.

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



802.1Q VLANs - Add

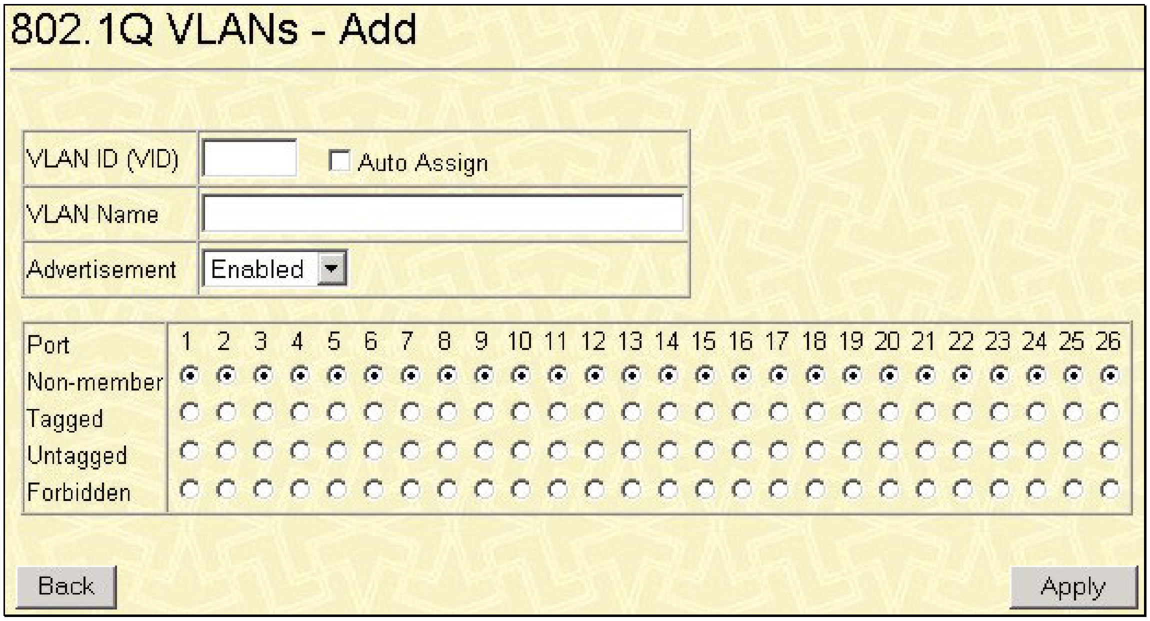
VLAN ID (VID)	□ Auto Assign
VLAN Name	
Advertisement	Enabled

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Non-member	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 6- 15. 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)



802.1Q VLANs - Add

VLAN ID (VID)	□ Auto Assign
VLAN Name	
Advertisement	Enabled

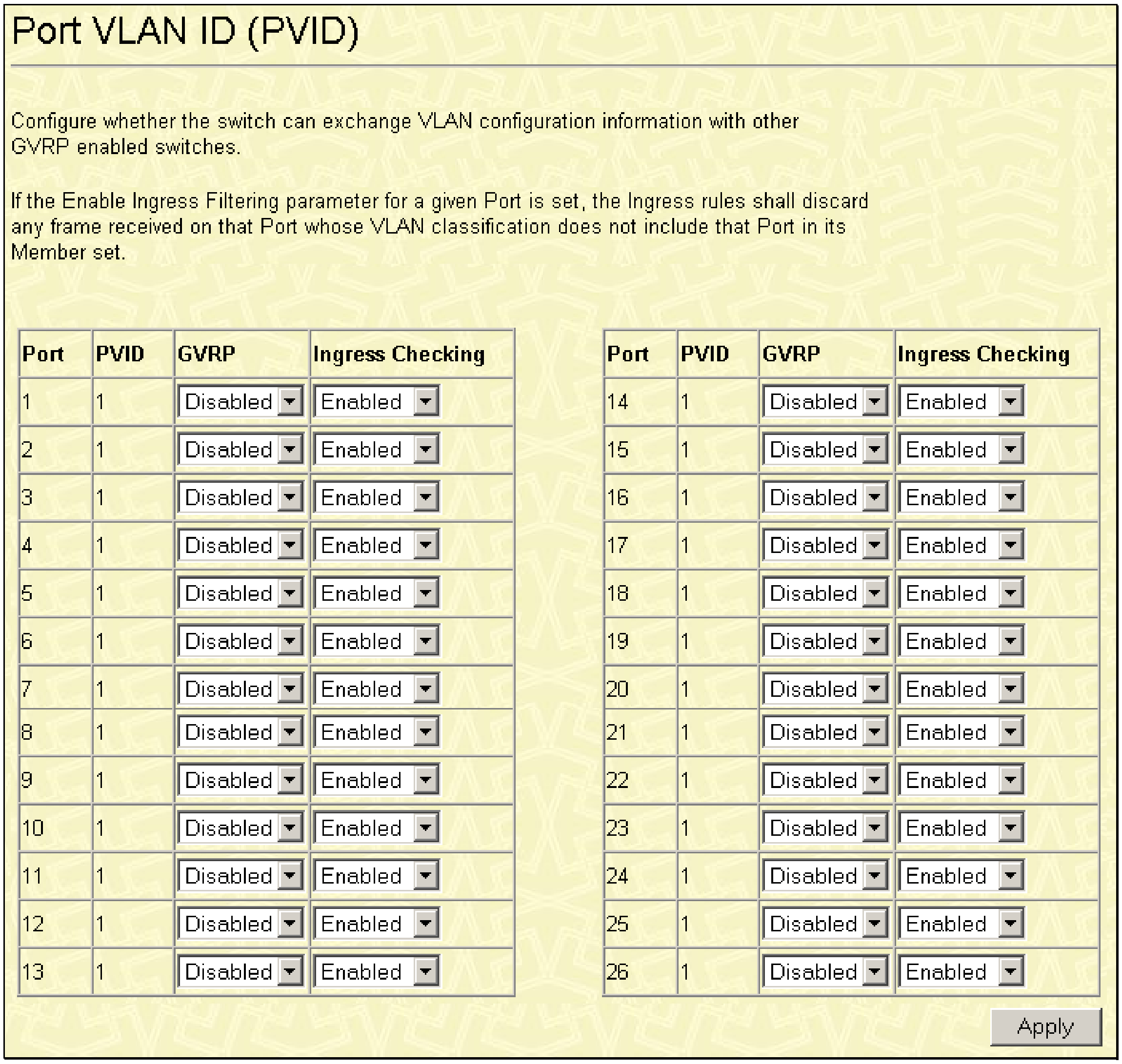
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Non-member	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 6- 16. 802.1Q VLANs – Add 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.

IEEE 802.1Q Port Settings



Port VLAN ID (PVID)

Configure whether the switch can exchange VLAN configuration information with other GVRP enabled switches.

If the Enable Ingress Filtering parameter for a given Port is set, the Ingress rules shall discard any frame received on that Port whose VLAN classification does not include that Port in its Member set.

Port	PVID	GVRP	Ingress Checking	Port	PVID	GVRP	Ingress Checking
1	1	Disabled	Enabled	14	1	Disabled	Enabled
2	1	Disabled	Enabled	15	1	Disabled	Enabled
3	1	Disabled	Enabled	16	1	Disabled	Enabled
4	1	Disabled	Enabled	17	1	Disabled	Enabled
5	1	Disabled	Enabled	18	1	Disabled	Enabled
6	1	Disabled	Enabled	19	1	Disabled	Enabled
7	1	Disabled	Enabled	20	1	Disabled	Enabled
8	1	Disabled	Enabled	21	1	Disabled	Enabled
9	1	Disabled	Enabled	22	1	Disabled	Enabled
10	1	Disabled	Enabled	23	1	Disabled	Enabled
11	1	Disabled	Enabled	24	1	Disabled	Enabled
12	1	Disabled	Enabled	25	1	Disabled	Enabled
13	1	Disabled	Enabled	26	1	Disabled	Enabled

Figure 6- 17. 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.

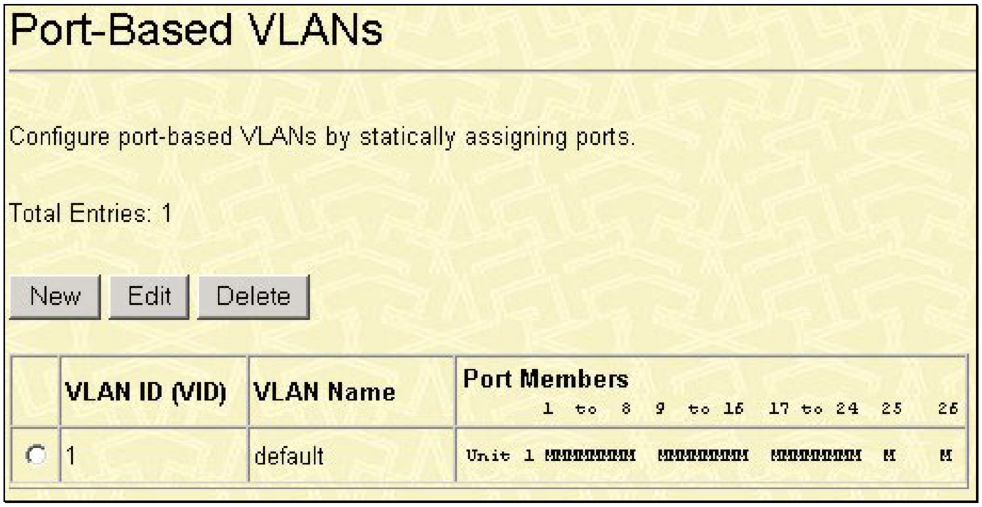
The information on the window is described as follows:

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.

Port-Based VLANs

If you have chosen **Port-Based VLAN**, the heading **Port-Based VLAN** will appear in the **VLAN Configuration** folder. Clicking on this folder will open the following screen:



Port-Based VLANs

Configure port-based VLANs by statically assigning ports.

Total Entries: 1

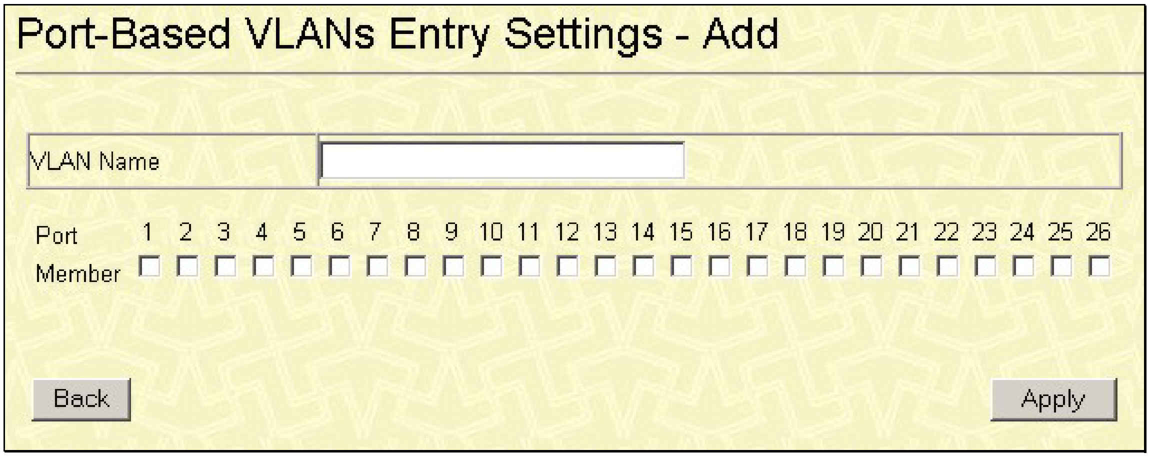
	VLAN ID (VID)	VLAN Name	Port Members 1 to 8 9 to 16 17 to 24 25 26
○	1	default	Unit 1 MMMMMMMM MMMMMMMM MMMMMMMM M M

Figure 6- 18. Port-Based VLANs window

The **Port-Based VLAN** screen shows the following information:

Parameter	Description
VLAN ID	The VLAN ID of the VLAN that was created.
VLAN Name	The name of the VLAN that is being created.
Port Members	Corresponds to the ports that are members of the particular VLAN.

To create a **Port-based VLAN,** click **NEW,** revealing the following screen.



Port-Based VLANs Entry Settings - Add

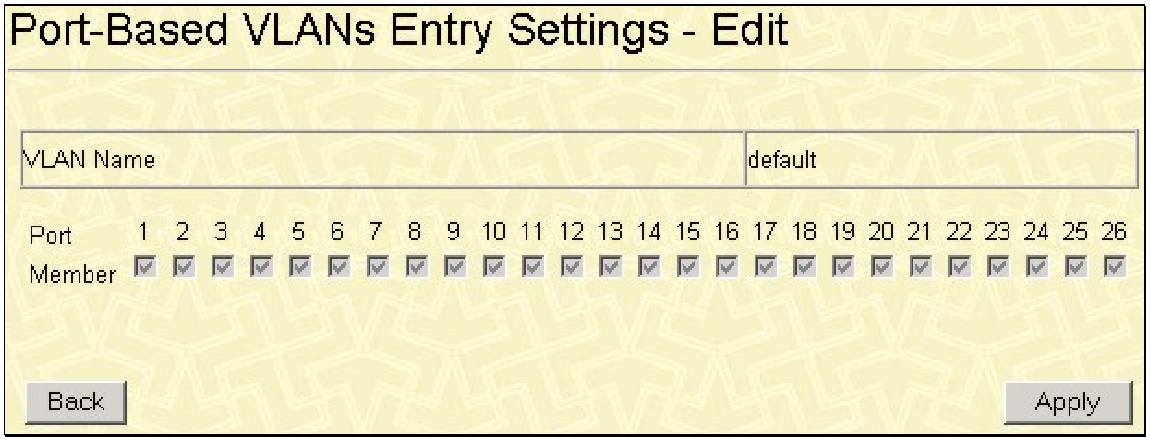
VLAN Name:

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

Figure 6- 19. Port-Based VLANs Entry Settings – Add

Enter a VLAN name in the **VLAN Name** field. Now decide which ports will be members of the VLAN by checking the corresponding port numbers. Press **Apply** to save your changes and click **Back** to return to the **Port-Based VLAN** screen.

To edit an existing entry, click the corresponding radio button of the VLAN entry and press the Edit button, revealing the following screen:



Port-Based VLANs Entry Settings - Edit

VLAN Name: default

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

Figure 6- 20. Port-Based VLANs entry Settings Edit window

After altering the Port Members of your Port-Based VLAN entry, click Apply to let your changes take effect.

Link Aggregation

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 DES-3226L supports up to 7 port trunk groups with 2 to 4 ports in each group. A potential bit rate of 800 Mbps can be achieved.

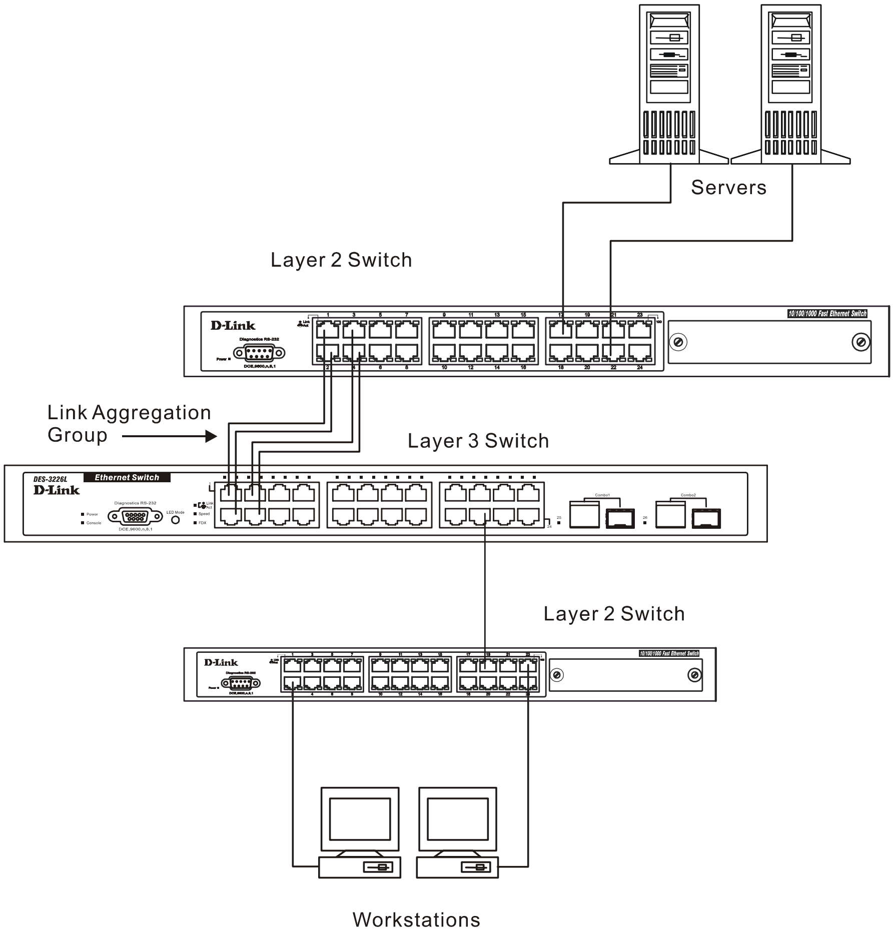


Figure 6- 21.. Example of Port Trunk Group

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.

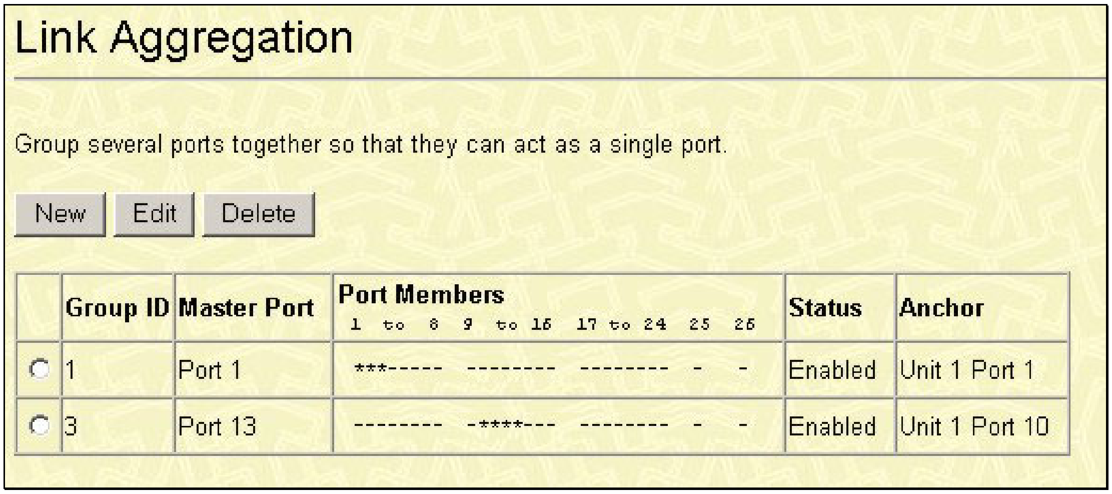
The switch allows the creation of up to 7 link aggregation groups, each group consisting of up of up to 4 links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the two (optional) Gigabit ports, which can only belong to a single link aggregation group. 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.

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:



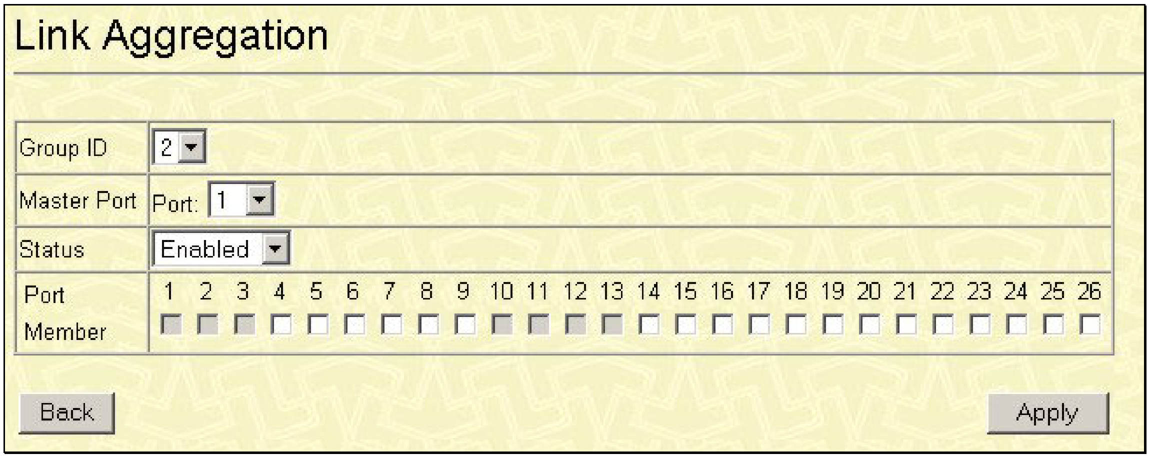
Link Aggregation

Group several ports together so that they can act as a single port.

	Group ID	Master Port	Port Members 1 to 8 9 to 16 17 to 24 25 26	Status	Anchor
○	1	Port 1	***----- -------- -------- - -	Enabled	Unit 1 Port 1
○	3	Port 13	-------- -****--- -------- - -	Enabled	Unit 1 Port 10

Figure 6- 22. Link Aggregation window

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



Link Aggregation

Group ID	2
Master Port	Port: 1
Status	Enabled
Port Member	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 □

Figure 6- 23. Link Aggregation add 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.
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.
Port Member	Allows the specification of the ports that will make up the link aggregation group.

802.1x

Understanding 802.1x Port-based Network Access Control

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

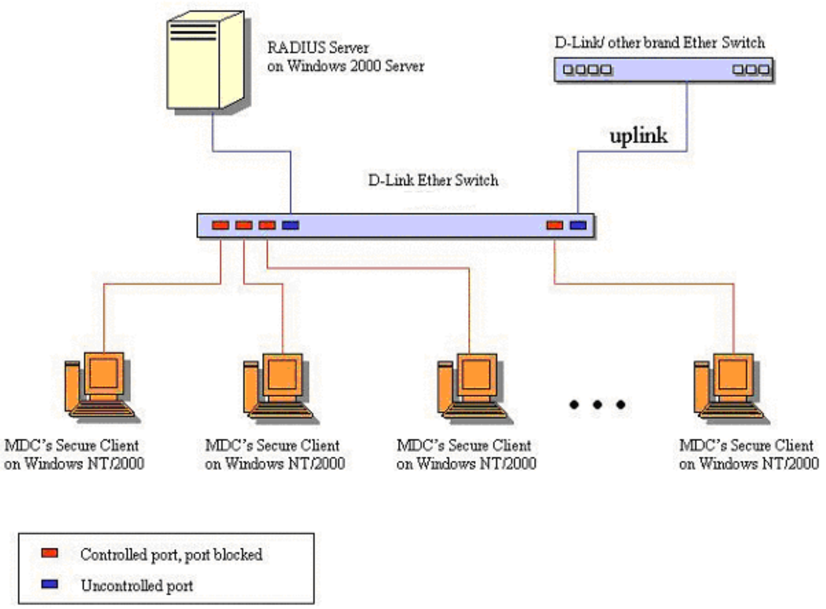
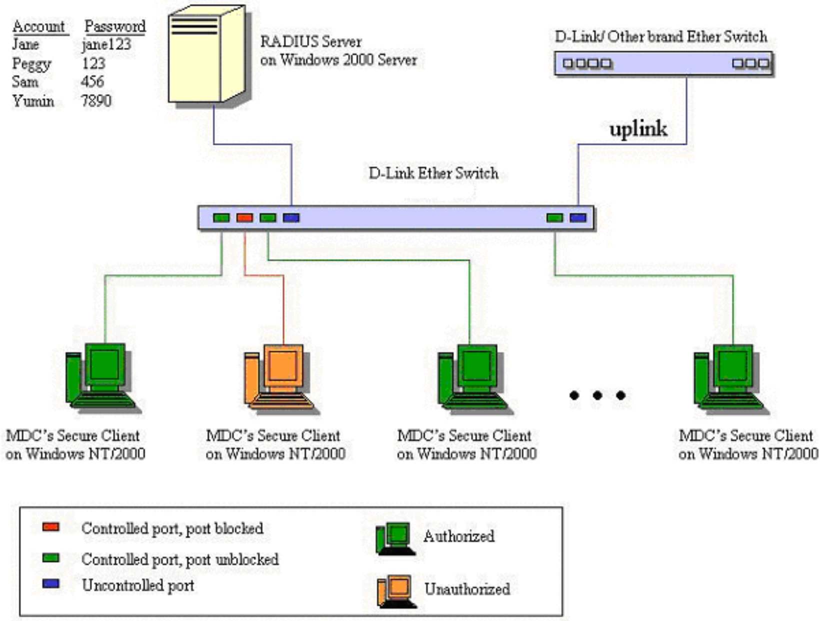


Figure 6- 24. Typical 802.1x Configuration Prior to User Authentication

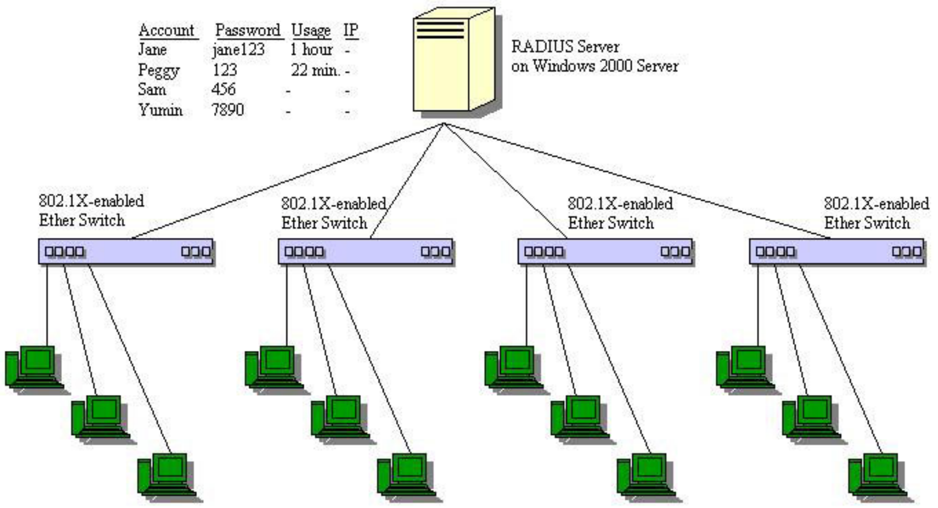
Once the user is authenticated, the Switch unblocks the port that is connected to the user as shown in the next figure.



Account	Password
Jane	jane123
Peggy	123
Sam	456
Yumin	7890

Figure 6- 25. 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.



Account	Password	Usage	IP
Jane	jane123	1 hour	-
Peggy	123	22 min.	-
Sam	456	-	-
Yumin	7890	-	-

Figure 6- 26. Typical Configuration with 802.1x Fully Implemented

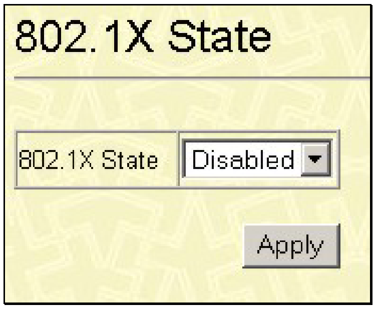
State Machine Name
Port Timers state machine
Authenticator PAE state machine
The Authenticator Key Transmit state machine
Reauthentication Timer state machine
Backend Authentication state machine
Controlled Directions state machine
The Key Receive state machine

Table 6- 2. Conformance to IEEE 802.1x Standards

The DES-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.

802.1x State



802.1X State

802.1X State: Disabled

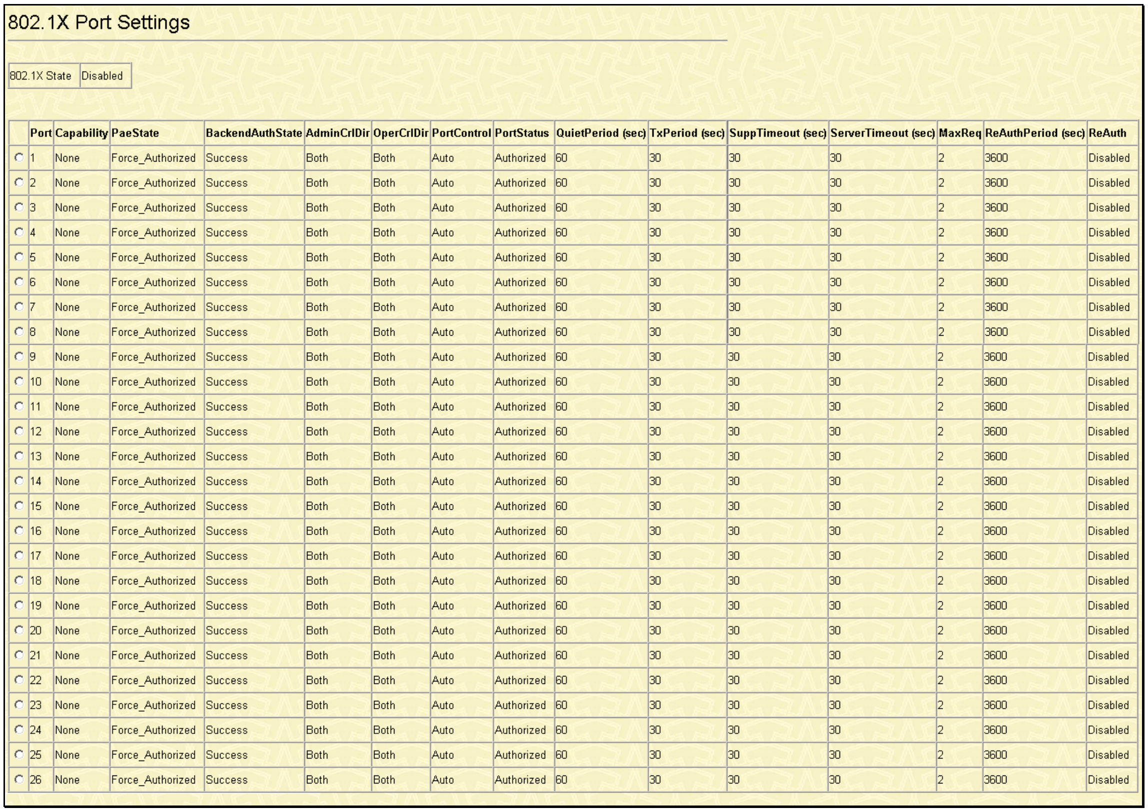
Figure 6- 27. 802.1x State window

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.

802.1x Port Settings

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



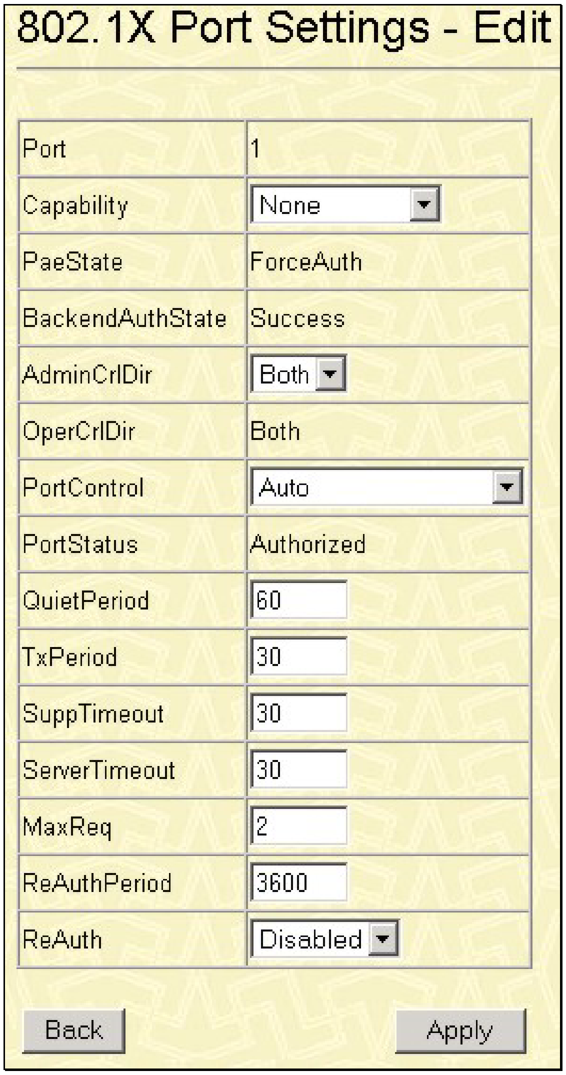
802.1X Port Settings

802.1X State	Disabled

	Port	Capability	PaeState	BackendAuthState	AdminCrlDir	OperCrlDir	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 6- 28. 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. The following window will appear:



802.1X Port Settings - Edit

Port	1
Capability	None
PaeState	ForceAuth
BackendAuthState	Success
AdminCrlDir	Both
OperCrlDir	Both
PortControl	Auto
PortStatus	Authorized
QuietPeriod	60
TxPeriod	30
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled

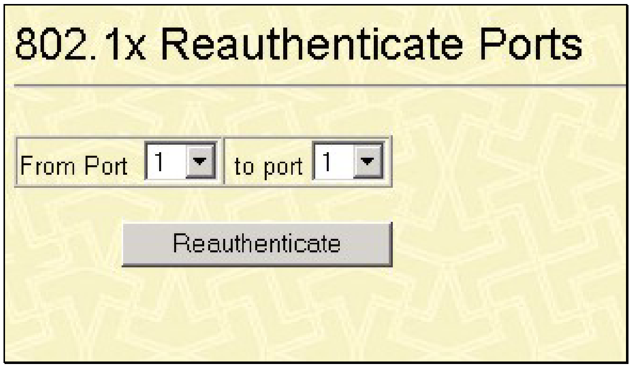
Figure 6- 29. 802.1x Port Settings – Edit window

Configure the following 802.1x port settings:

Parameter	Description
Port	Port being configured for 802.1x settings.
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.
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.

802.1X Reauthenticate Ports



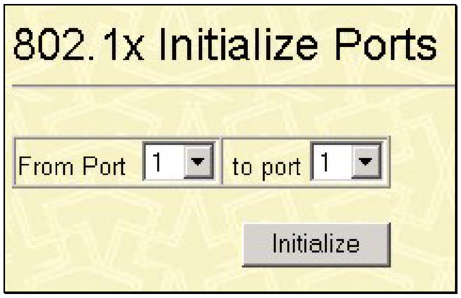
802.1x Reauthenticate Ports

From Port 1 to port 1

Figure 6- 30. 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.

802.1X Initialize Ports



802.1x Initialize Ports

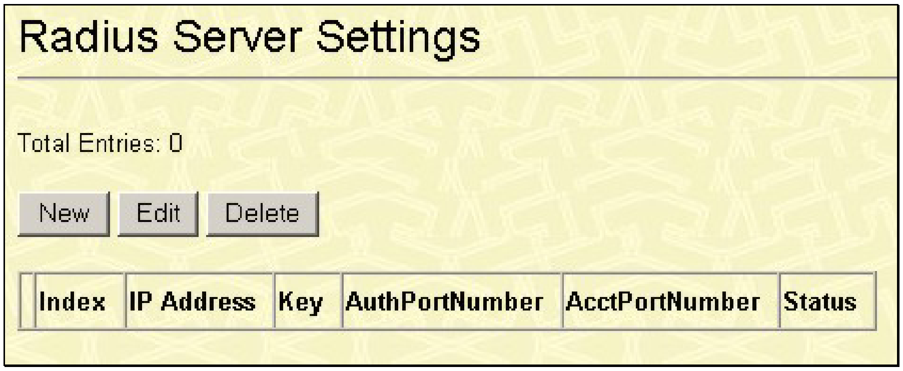
From Port 1 to port 1

Figure 6- 31. 802.1X Initialize Ports window.

This screen allows you to initializethe 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.

RADIUS Server Settings

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



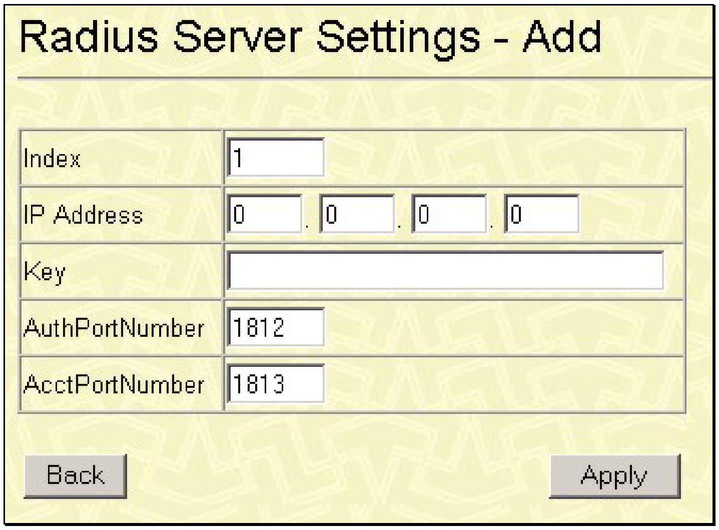
Radius Server Settings

Total Entries: 0

	Index	IP Address	Key	AuthPortNumber	AcctPortNumber	Status

Figure 6- 32. 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.



Radius Server Settings - Add

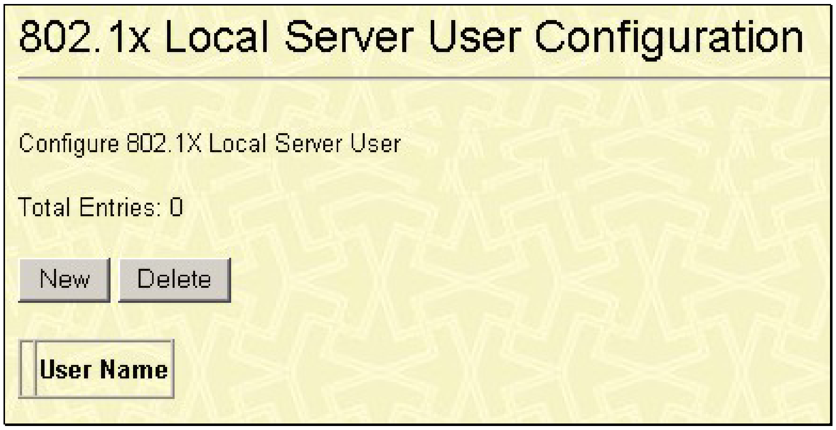
Index	1
IP Address	0 . 0 . 0 . 0
Key	
AuthPortNumber	1812
AcctPortNumber	1813

Figure 6- 33. 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.

Local Server User



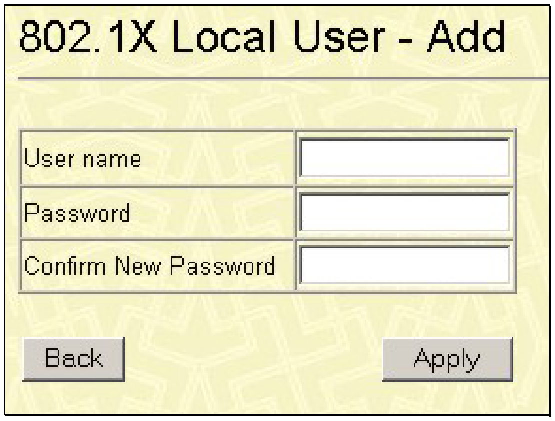
802.1x Local Server User Configuration

Configure 802.1X Local Server User

Total Entries: 0

Figure 6- 34. 802.1x Local Server User Configuration window

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



802.1X Local User - Add

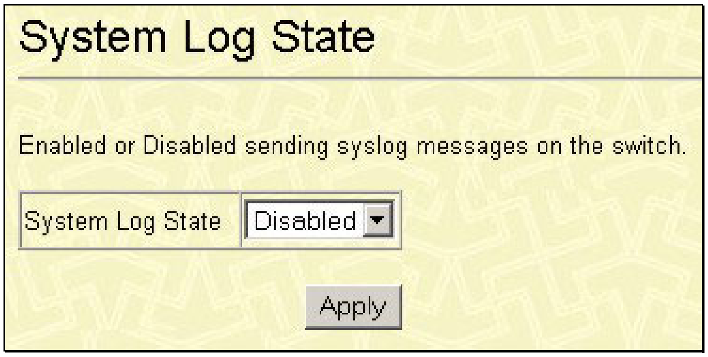
User name	
Password	
Confirm New Password	

Figure 6- 35. 802.1x Local User – Add window

System Log

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

System Log State



System Log State

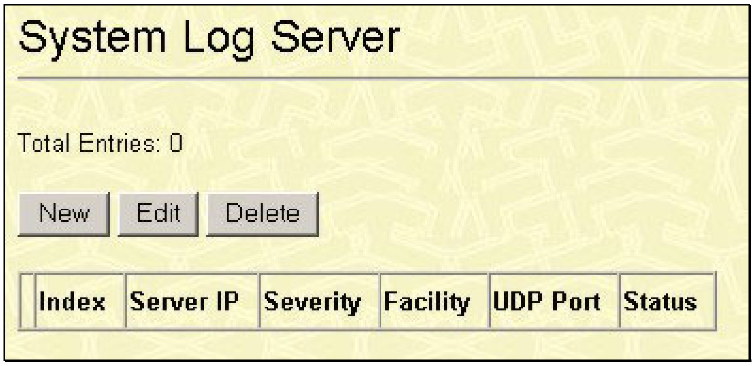
Enabled or Disabled sending syslog messages on the switch.

System Log State: Disabled

Figure 6- 36. 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.

System Log Server



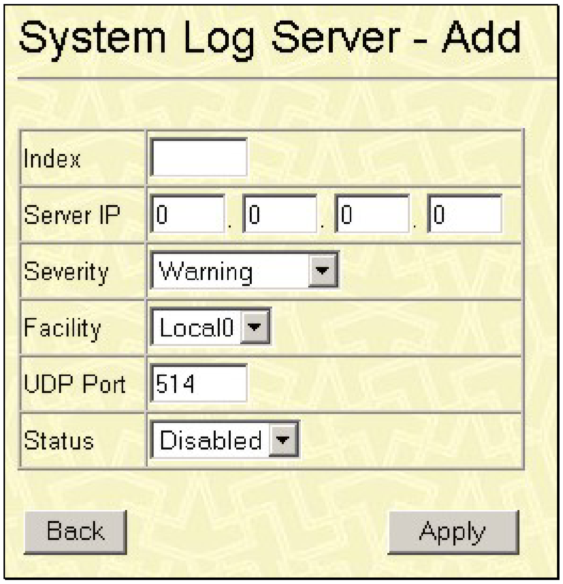
System Log Server

Total Entries: 0

Index	Server IP	Severity	Facility	UDP Port	Status

Figure 6- 37. System Log Server window

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



System Log Server - Add

Index	
Server IP	0 . 0 . 0 . 0
Severity	Warning
Facility	Local0
UDP Port	514
Status	Disabled

Figure 6- 38. 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*.
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.

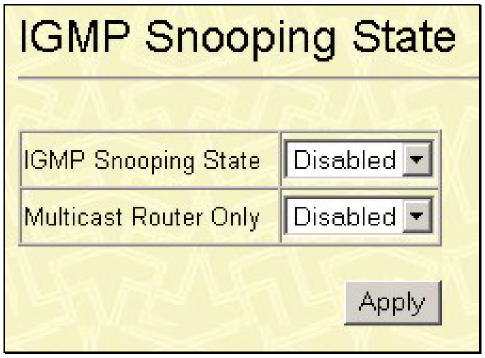
Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon

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.

Multicast Configuration

IGMP Snooping Global



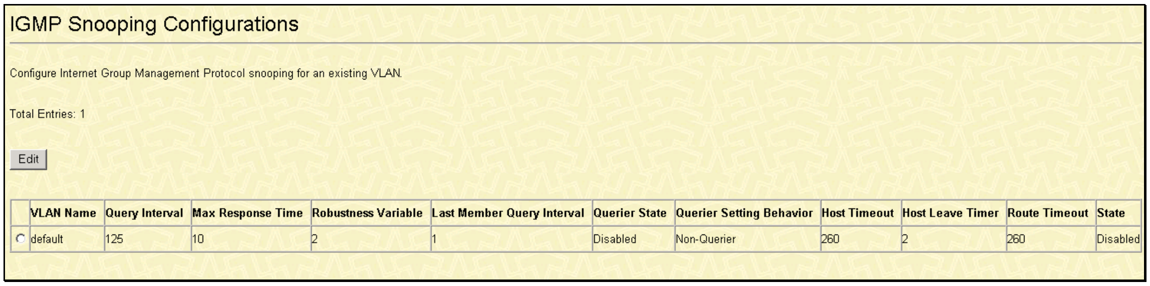
IGMP Snooping State

IGMP Snooping State	Disabled
Multicast Router Only	Disabled

Figure 6- 39. 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.

IGMP Snooping Configurations



IGMP Snooping Configurations

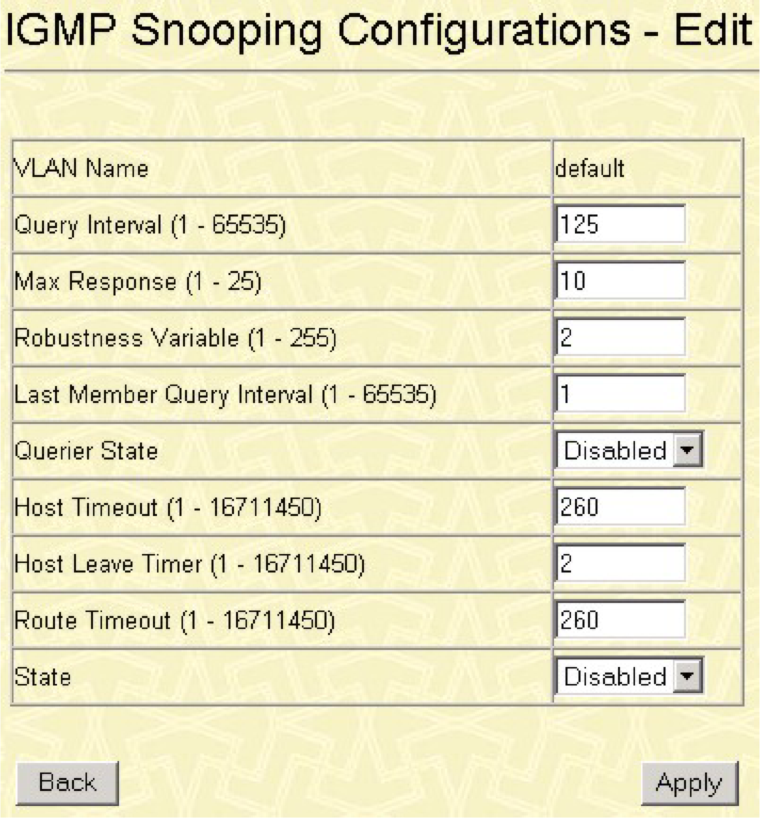
Configure Internet Group Management Protocol snooping for an existing VLAN.

Total Entries: 1

	VLAN Name	Query Interval	Max Response Time	Robustness Variable	Last Member Query Interval	Querier State	Querier Setting Behavior	Host Timeout	Host Leave Timer	Route Timeout	State
○	default	125	10	2	1	Disabled	Non-Querier	260	2	260	Disabled

Figure 6- 40. IGMP Snooping Configurations window

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



IGMP Snooping Configurations - Edit

VLAN Name	default
Query Interval (1 - 65535)	125
Max Response (1 - 25)	10
Robustness Variable (1 - 255)	2
Last Member Query Interval (1 - 65535)	1
Querier State	Disabled
Host Timeout (1 - 16711450)	260
Host Leave Timer (1 - 16711450)	2
Route Timeout (1 - 16711450)	260
State	Disabled

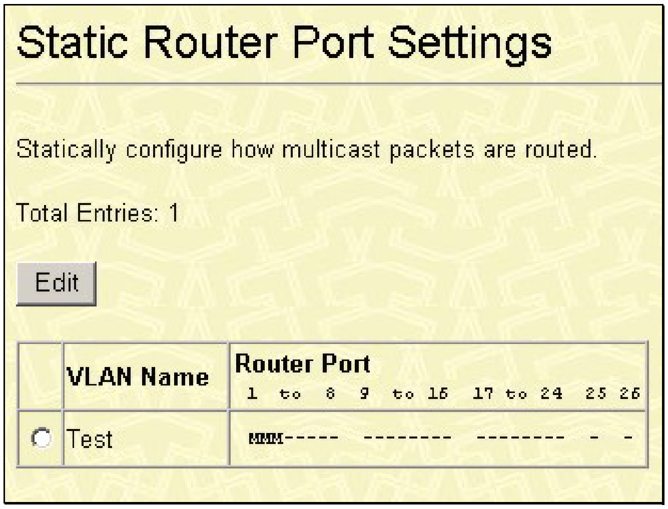
Figure 6- 41. IGMP Snooping Configurations – Edit window

The following parameters can be set:

Parameter	Description
Query Interval	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	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	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	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	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.
Host Leave Timer	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	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.

Static Router Port Settings



Static Router Port Settings

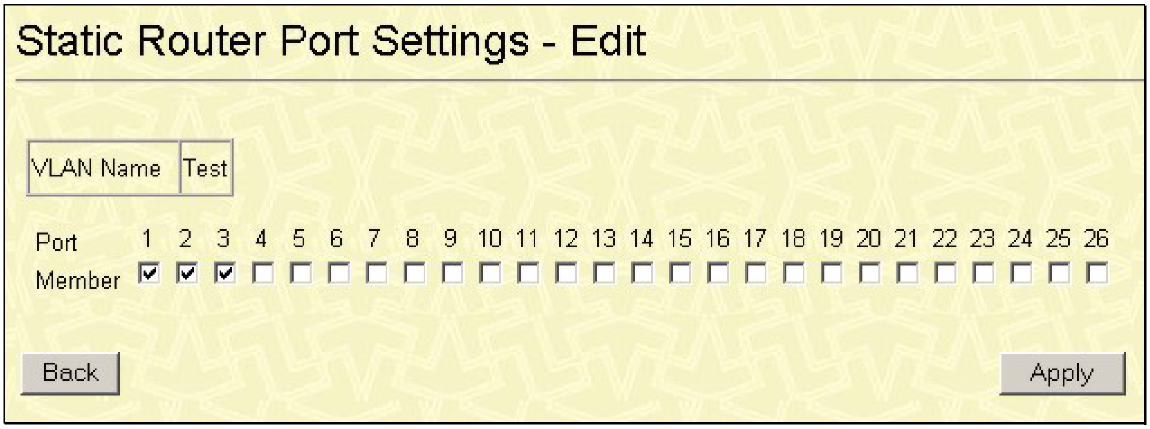
Statically configure how multicast packets are routed.

Total Entries: 1

	VLAN Name	Router Port 1 to 8 9 to 16 17 to 24 25 26
○	Test	MMM----- -------- -------- - -

Figure 6- 42. Static Router Port Settings window

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



Static Router Port Settings - Edit

VLAN Name	Test

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

Figure 6- 43. Static Router Port Settings – Edit window

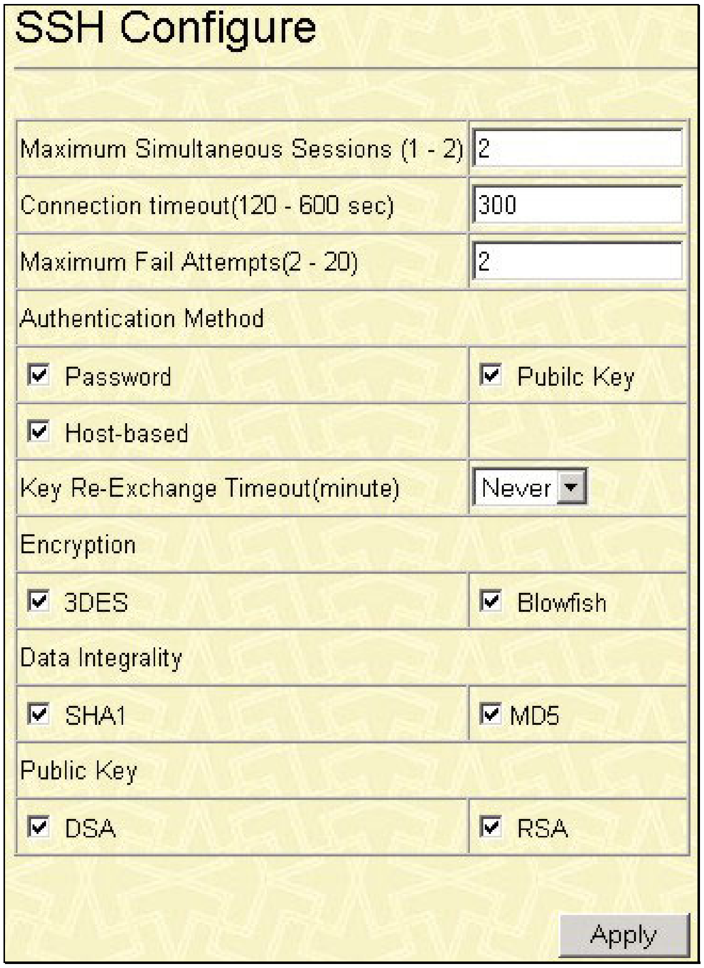
SSH Management

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.

SSH Global



SSH Configure

Maximum Simultaneous Sessions (1 - 2)	2
Connection timeout(120 - 600 sec)	300
Maximum Fail Attempts(2 - 20)	2
Authentication Method	
☑ Password	☑ Pubilc Key
☑ Host-based	
Key Re-Exchange Timeout(minute)	Never ▾
Encryption	
☑ 3DES	☑ Blowfish
Data Integrality	
☑ SHA1	☑ MD5
Public Key	
☑ DSA	☑ RSA

Figure 6- 44. SSH Configure window

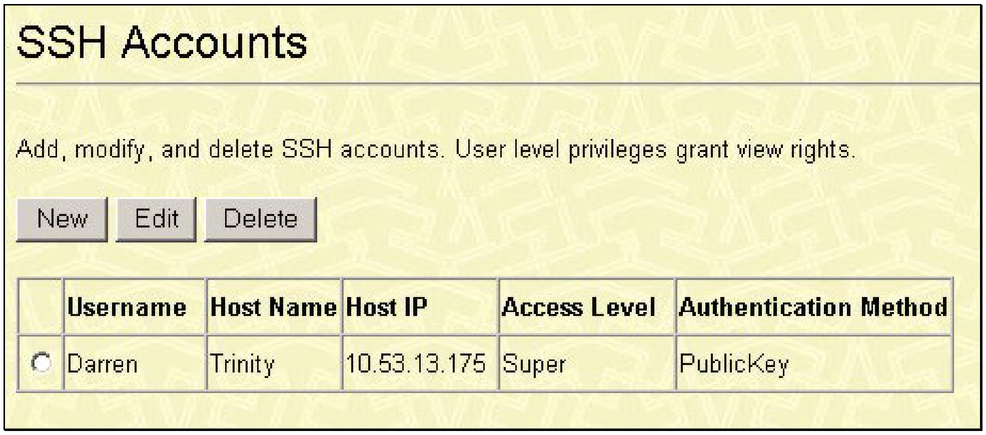
The **SSH Configure** window contains the global server setting: maximum simultaneous sessions, connection timeout, maximum fail attempts, authentication method, key re-exchange timeout, the encryption algorithms, data integrality algorithms and public key algorithms.

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	Specify the maximum number of allowed authentication attempts before access

Attempts(2 – 20)	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.

SSH Account Configuration



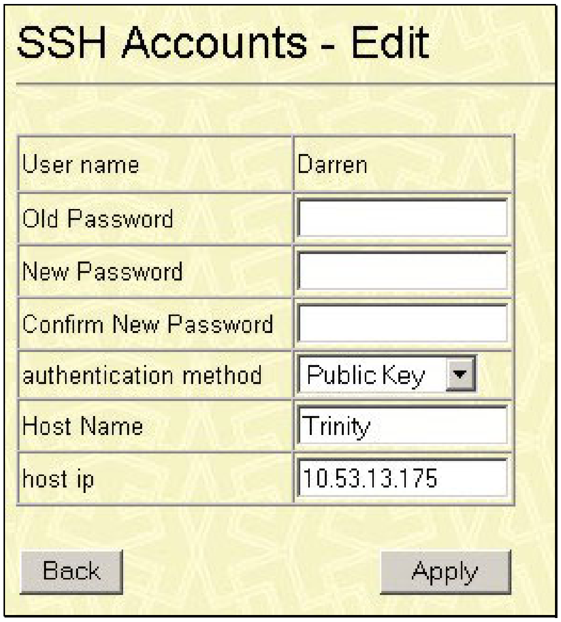
SSH Accounts

Add, modify, and delete SSH accounts. User level privileges grant view rights.

	Username	Host Name	Host IP	Access Level	Authentication Method
○	Darren	Trinity	10.53.13.175	Super	PublicKey

Figure 6- 45. SSH Accounts window

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



SSH Accounts - Edit

User name	Darren
Old Password	
New Password	
Confirm New Password	
authentication method	Public Key ▾
Host Name	Trinity
host ip	10.53.13.175

Figure 6- 46. 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.

Appendix A

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

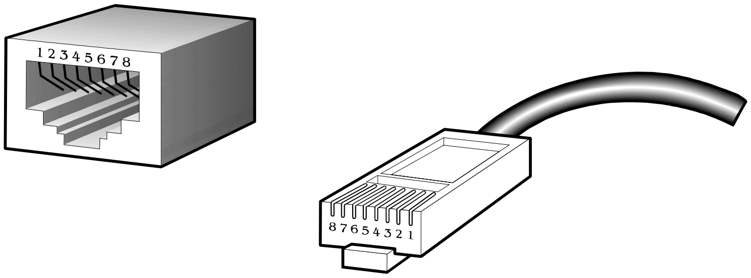
Performance

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

Appendix B

Cables and Connectors

When connecting the Switch to another switch, a bridge or hub, a normal cable is necessary. Please review these products for matching cable pin assignment.
The following diagrams and tables show the standard RJ-45 receptacle/connector and their pin assignments.



The standard RJ-45 port and connector

RJ-45 Pin Assignments		
Contact	**MDI-X Port**	**MDI-II Port**
1	RD+ (receive)	TD+ (transmit)
2	RD- (receive)	TD- (transmit)
3	TD+ (transmit)	RD+ (receive)
4	Not used	Not used
5	Not used	Not used
6	TD- (transmit)	RD- (receive)
7	Not used	Not used
8	Not used	Not used

The standard RJ-45 pin assignments

Appendix C

Cable Lengths

Use the following table to as a guide for the maximum 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

Glossary

1000BASE-LX: A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters

1000BASE-SX: A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers

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.

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.

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.

D-Link Offices

Australia
D-Link Australasia
1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia
TEL: 61-2-8899-1800 FAX: 61-2-8899-1868
TOLL FREE (Australia): 1300 766 868
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au & info@dlink.com.au

Brazil
D-Link Brasil Ltda.
Rua Tavares Cabral 102 - Conj. 31 e 33
05423-030 Pinheiros, Sao Paulo, Brasil
TEL: (5511) 3094 2910 to 2920 FAX: (5511) 3094 2921
URL: www.dlink.com.br

Canada
D-Link Canada
2180 Winston Park Drive, Oakville,
Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223
BBS: 1-965-279-8732 FTP: ftp.dlinknet.com
TOLL FREE: 1-800-354-6522
URL: www.dlink.ca E-MAIL: techsup@dlink.ca

Chile
D-Link South America (Sudamérica)
Isidora Goyenechea 2934
Oficina 702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-232-0923
URL: www.dlink.com.cl

China
D-Link Beijing
Level 5,Tower W1,The Tower,Oriental Plaza
No.1,East Chang An Ave., Dong Cheng District
Beijing,100738,China
TEL: (8610) 85182529/30/31/32/33
FAX: (8610) 85182250
URL: www.dlink.com.cn E-MAIL: webmaster@dlink.com.cn

Denmark
D-Link Denmark
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL: 45-43-969040 FAX: 45-43-424347
URL: www.dlink.dk E-MAIL: info@dlink.dk

Egypt
D-Link Middle East
7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt
TEL: 202-624-4615 FAX: 202-624-583
URL: www.dlink-me.com
E-MAIL: support@dlink-me.com & dlinkegypt@dlink-me.com

Finland
D-Link Finland
Pakkalankuja 7A, 01510 Vantaa, Finland
TEL: 358-9-2707-5080 FAX: 358-9-2707-5081
URL: www.dlink-fi.com

France
D-Link France
Le Florilege, No. 2, Allée de la Fresnerie,
78330 Fontenay-le-Fleury, France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689
URL: www.dlink-france.fr
E-MAIL: info@dlink-france.fr

Germany
D-Link Central Europe (D-Link Deutschland GmbH)
Schwalbacher Strasse 74, D-65760 Eschborn, Germany
TEL: 49-6196-77990 FAX: 49-6196-7799300
BBS: 49-(0) 6192-971199 (analog) & BBS: 49-(0) 6192-971198 (ISDN)
INFO: 00800-7250-0000 (toll free) & HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 & HELP: support.dlink.de
URL: www.dlink.de & E-MAIL: info@dlink.de

India
D-Link India
Plot No.5, Kurla -Bandra Complex Rd., Off Cst Rd.,
Santacruz (East), Mumbai, 400 098 India
TEL: 91-022-2652-6696/6788/6623
FAX: 91-022-2652-8914/8476
URL: www.dlink.co.in
E-MAIL: service@dlink.co.in & tushars@dlink.co.in

Italy
D-Link Mediterraneo Srl/D-Link Italia
Via Nino Bonnet n. 6/B, 20154, Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723
URL: www.dlink.it E-MAIL: info@dlink.it

Japan
D-Link Japan
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868
URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp

Netherlands
D-Link Benelux
Lichtenauerlaan 102-120, 3062 ME Rotterdam, Netherlands
TEL: +31-10-2045740 FAX: +31-10-2045880
URL: www.d-link-benelux.nl & www.dlink-benelux.be
E-MAIL: info@dlink-benelux.com

Norway
D-Link Norway
Karihaugveien 89, 1086 Oslo
TEL: 47-22-309075 FAX: 47-22-309085
SUPPORT: 800-10-610 & 800-10-240 (DI-xxx)
URL: www.dlink.no

Russia
D-Link Russia
129626 Russia, Moscow, Graphskiy per., 14, floor 6
TEL/FAX: +7 (095) 744-00-99
URL: www.dlink.ru E-MAIL: vl@dlink.ru

Singapore
D-Link International
1 International Business Park, #03-12 The Synergy,
Singapore 609917
TEL: 65-6774-6233 FAX: 65-6774-6322
E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

South Africa
D-Link South Africa
Einstein Park II, Block B, 102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion, Gauteng, Republic of South Africa
TEL: +27-12-665-2165 FAX: +27-12-665-2186
URL: www.d-link.co.za E-MAIL: attie@d-link.co.za

Spain
D-Link Iberia S.L.
Sabino de Arana, 56 bajos, 08028 Barcelona, Spain
TEL: 34 93 409 0770 FAX: 34 93 491 0795
URL: www.dlink.es E-MAIL: info@dlink.es

Sweden
D-Link Sweden
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-8-564-61900 FAX: 46-8-564-61901
URL: www.dlink.se E-MAIL: info@dlink.se

Taiwan
D-Link Taiwan
2F, No. 119, Pao-chung Road, Hsin-tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw E-MAIL: dssqa@dlinktw.com.tw

Turkey
D-Link Turkiye
Beybi Giz Plaza, Ayazaga Mah. Meydan Sok. No. 28
Maslak 34396, Istanbul-Turkiye
TEL: 90-212-335-2553 (direct) & 90-212-335-2525 (pbx)
FAX: 90-212-335-2500 E-MAIL: dlinkturkey@dlink-me.com
E-MAIL: support@dlink-me.com

U.A.E. **D-Link Middle East FZCO**
P.O. Box18224 R/8, Warehouse UB-5
Jebel Ali Free Zone, Dubai – United Arab Emirates
TEL: (Jebel Ali): 971-4-883-4234
FAX: (Jebel Ali): 971-4-883-4394 & (Dubai): 971-4-335-2464
E-MAIL: dlinkme@dlink-me.com & support@dlink-me.com

U.K. **D-Link Europe (United Kingdom) Ltd**
4th Floor, Merit House, Edgware Road, Colindale, London
NW9 5AB United Kingdom
TEL: 44-020-8731-5555 SALES: 44-020-8731-5550
FAX: 44-020-8731-5511 SALES: 44-020-8731-5551
BBS: 44 (0) 181-235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. **D-Link U.S.A.**
17595 Mt. Hermmann, Fountain Valley, CA 92708 USA
TEL: 1-714-885-6000 FAX: 1-866-743-4905
INFO: 1-877-453-5465 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com

Warranty and Registration for all Countries and Regions Except USA

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sint beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS.

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

Limited Warranty (USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

Limited Lifetime Warranty for the Product(s) is defined as follows:

- Hardware for as long as the original customer/end user owns the product, or five years after product discontinuance, whichever occurs first (excluding power supplies and fans)
- Power Supplies and Fans Three (3) Year
- Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.

The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 53 Discovery Drive, Irvine, CA 92618**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective manufacturers or owners.

Copyright Statement: No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright© 2002 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures**:**

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty outside the United States, please contact corresponding local D-Link office.

Register online your D-Link product at
http://support.dlink.com/register/

Registration Card

Print, type or use block letters.

Your name: Mr./Ms____

Organization: ________________________________Dept.____________________

Your title at organization:______________ Telephone:________________ Fax:__________

Organization's full address:______________________________________

Country:____

Date of purchase (Month/Day/Year):______________________________

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name:____

Telephone:_______________________ Fax:__________________________

Reseller's full address:______________________________________

____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
□Home □Office □Travel □Company Business □Home Business □Personal Use

2. How many employees work at installation site?
□1 employee □2-9 □10-49 □50-99 □100-499 □500-999 □1000 or more

3. What network protocol(s) does your organization use ?
□XNS/IPX □TCP/IP □DECnet □Others_________________________________

4. What network operating system(s) does your organization use ?
□D-Link LANsmart □Novell NetWare □NetWare Lite □SCO Unix/Xenix □PC NFS □3Com 3+Open
□Banyan Vines □DECnet Pathwork □Windows NT □Windows NTAS □Windows '95
□Others____

5. What network management program does your organization use ?
□D-View □HP OpenView/Windows □HP OpenView/Unix □SunNet Manager □Novell NMS
□NetView 6000 □Others____

6. What network medium/media does your organization use ?
□Fiber-optics □Thick coax Ethernet □Thin coax Ethernet □10BASE-T UTP/STP
□100BASE-TX □100BASE-T4 □100VGAnyLAN □Others__________________________

7. What applications are used on your network?
□Desktop publishing □Spreadsheet □Word processing □CAD/CAM □Database management □Accounting
□Others____

8. What category best describes your company?
□Aerospace □Engineering □Education □Finance □Hospital □Legal □Insurance/Real Estate □Manufacturing
□Retail/Chainstore/Wholesale □Government □Transportation/Utilities/Communication □VAR □System house/company □Other____________________________________

9. Would you recommend your D-Link product to a friend?
□Yes □No □Don't know yet

10.Your comments on this product? ___________________________________

____

____

____

____

PLEASE
PLACE STAMP
HERE

TO: ______________________

____

____

D-Link®