D-Link ™ DGS-3224SR

High-Density Stackable Gigabit Ethernet Switch

User's Guide

August 2003 P/N 651GS3224015

CONTENTS

Intended Readers

The *DGS-3224SR User Guide* contains information for setup and management and of the DGS-3224SR switch. This guide 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. Components inside these compartments should be serviced only by a trained service technician.

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.

Safety Instructions (continued)

- 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.

Safety Instructions (continued)

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

Switch Description

The DGS-3224SR is a modular Gigabit Ethernet backbone switch designed for adaptability and scalability. The switch provides a management platform and uplink to backbone for a stacked group of twelve DGS-3224SR Layer 2 switches in a ring or chain topology arrangement. Alternatively, the switch can utilize up to twelve Gigabit Ethernet ports to function as a central distribution hub for other switches or switch groups, or routers. The four built-in combination Gigabit ports have the option of being used as either 1000BASE-T or SFP Gigabit connections.

Features

- 4 built-in combination 1000BASE-T/SFP ports
- Ring or chain topology switch stacking configuration for up to 12 additional DES-3224SR switches
- 88 Gbps switching fabric capacity
- Supports 802.1D STP and 802.1w Rapid Spanning Tree for redundant back up bridge paths
- Supports 802.1Q VLAN, IGMP snooping, 802.1p Priority Queues, port trunking, port mirroring
- Multi-layer Access Control (based on MAC address, IP address, VLAN, Protocol, 802.1p, DSCP)
- Quality of Service (QoS) customized control
- 802.1x (port-based) access control and Radius Client support
- Administrator-definable port security
- Per-port bandwidth control
- IEEE 802.3z and IEEE 802.3x compliant Flow Control for all Gigabit ports
- SNMP v.1, v.2, v.3 network management, RMON support
- Support optional external Redundant Power Supply
- Supports Web-based management.
- CLI management support
- DHCP and BOOTP Client support.
- Fully configurable either in-band or out-of-band control via RS-232 console serial connection.
- Telnet remote control console
- TFTP upgrade
- Traffic Segmentation

- SysLog support
- Simple Network Time Protocol
- Web GUI Traffic Monitoring

Front-Panel Components

The front panel of the Switch consists of LED indicators, an RS-232 communication port, and four SFP (Mini-GBIC) combo ports.

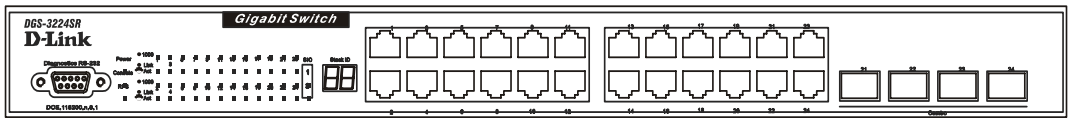


Figure 1 - 1. Front Panel View of the switch

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

An RS-232 DCE console port for setting up and managing the switch via a connection to a console terminal or PC using a terminal emulation program.

LED Indicators

The LED indicators of the Switch include Power, Master, Console, and RPS (Redundant Power Supply). A bank of 24 LEDs (2 for each port) indicates link, activity status and connection speed for each port

Power	It will light green approximately 2 seconds after the switch is powered on to indicate the ready state of the device.
Master	Lights steady green when the Switch is configured as the Master Switch in a stack.
Console	This indicator on the front panel should be lit during the Power-On Self Test (POST). Lights green when the switch is being managed via out-of-band/local console management through the RS-232 console port using a straight-through serial cable.
RPS	This indicator will light steady amber when an external power supply is supplying power. This indicates the internal power supply has failed.
1000 **Link/Act**	Each on-board Gigabit Ethernet port has a corresponding indicator. This will light steady green for a valid link and blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.
Stack ID	The switch includes a 7-segment LED (labeled **STACK ID**) to indicate the switch status in a stacked switch group.
SIO	Indicates which stacking port, if any, is in use.

Rear Panel Description

The rear panel of the switch contains an AC power connector, a connector for the Redundant Power Supply (RPS) and two stacking ports.

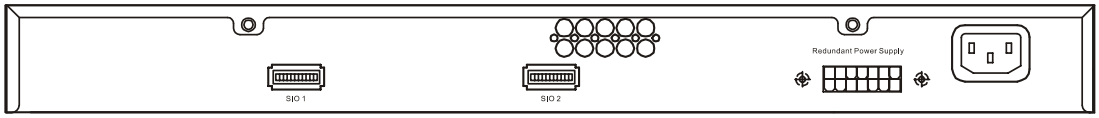


Figure 1-2. Rear panel view of the Switch

The AC power connector is a standard three-pronged connector that supports the power cord. Plug 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.

RPS Connector

Connect the optional external redundant power supply to the RPS connector. If the switch's internal power unit fails, the redundant power system automatically supplies power to the switch for uninterrupted operation.
The switch supports the D-Link RPS-500 redundant power supply units.

Management Options

The system may be managed out-of-band through the console port on the front panel or in-band using Telnet or 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).

NOTE: To access the switch through a web browser, the computer running the web browser must have IP-based network access to the switch.

Command Line Console Interface Through the Serial Port or Telnet

You can also connect a computer or terminal to the serial console port or use Telnet to access the switch. The command-line-driven interface provides complete access to all switch management features. For a full list of commands, see the *Command Line Reference*, which is included on the documentation CD.

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.

The switch supports a comprehensive set of MIB extensions:

- RFC1213 MIB II
- RFC1493 Bridge
- RFC1757 RMON
- RFC 1643 Ether-like MIB
- D-Link Enterprise MIB
- 802.1p RFC2674
- RFC 2233 Interface MIB
- RFC 1907 (SNMPv2-MIB)
- RSTP-MIB
- RFC2021 (RMON2)
- RFC2571 (SNMP Frameworks)
- RFC2572 (Message Processing for SNMP)
- RFC2573 (SNMP Applications)
- RFC2574 (USM for SNMP)
- RFC 2618 (Radius-Auth-Client-MIB)
- RFC 2620 (Radius-Acc-Client-MIB)
- IEEE8021-PAE-MIB
- RFC2575 (VACM for SNMP)
- RFC2576 (Coexistence between SNMPs)

Section 2

Installation

Package Contents

Before you begin installing the switch, confirm that your package contains the following items:

- One DGS-3224SR Layer 2 Gigabit Switch
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This User's Guide with Registration Card
- CLI Reference
- CD-ROM with User's Guide and CLI Reference

Before You Connect to the Network

NOTICE: Do not connect the switch to the network until you have established the correct IP settings.

Before you connect to the network, you must install the switch on a flat surface or in a rack, set up a terminal emulation program, plug in the power cord, and then set up a password and IP address.

The switch is supplied with rubber feet for stationing it on a flat surface and mounting brackets and screws for mounting the switch in a rack.

NOTICE: Do not connect the stacked switch group to the network until you have properly configured all switches for switch stacking. An improperly configured switch stack can cause a broadcast storm.

Installing the Switch Without the Rack

1. Install the switch on a level surface that can safely support the weight of the switch and its attached cables. The switch must have adequate space for ventilation and for accessing cable connectors.
2. Set the switch on a flat surface and check for proper ventilation. Allow at least 5 cm (2 inches) on each side of the switch and 15 cm (6 inches) at the back for the power cable.
3. Attach the rubber feet on the marked locations on the bottom of the chassis.
4. The rubber feet, although optional, are recommended to keep the unit from slipping.

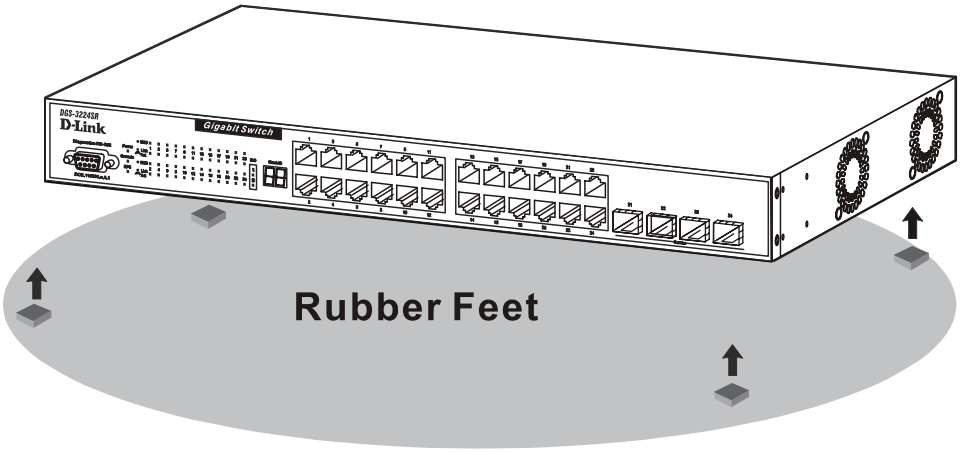


Figure 2-1. Install rubber feet for installations with or without a rack

Installing the Switch in a Rack

You can install the switch in most standard 19-inch (48.3-cm) racks. Refer to the illustrations below.

1. Use the supplied screws to attach a mounting bracket to each side of the switch.
2. Align the holes in the mounting bracket with the holes in the rack.
3. Insert and tighten two screws through each of the mounting brackets.

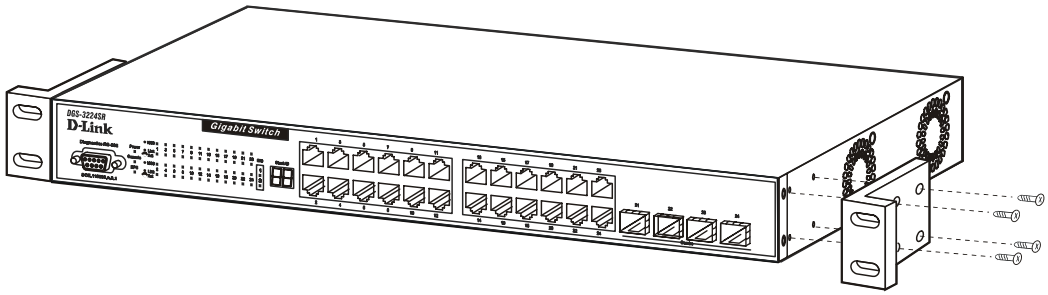


Figure 2-2. Attach mounting brackets

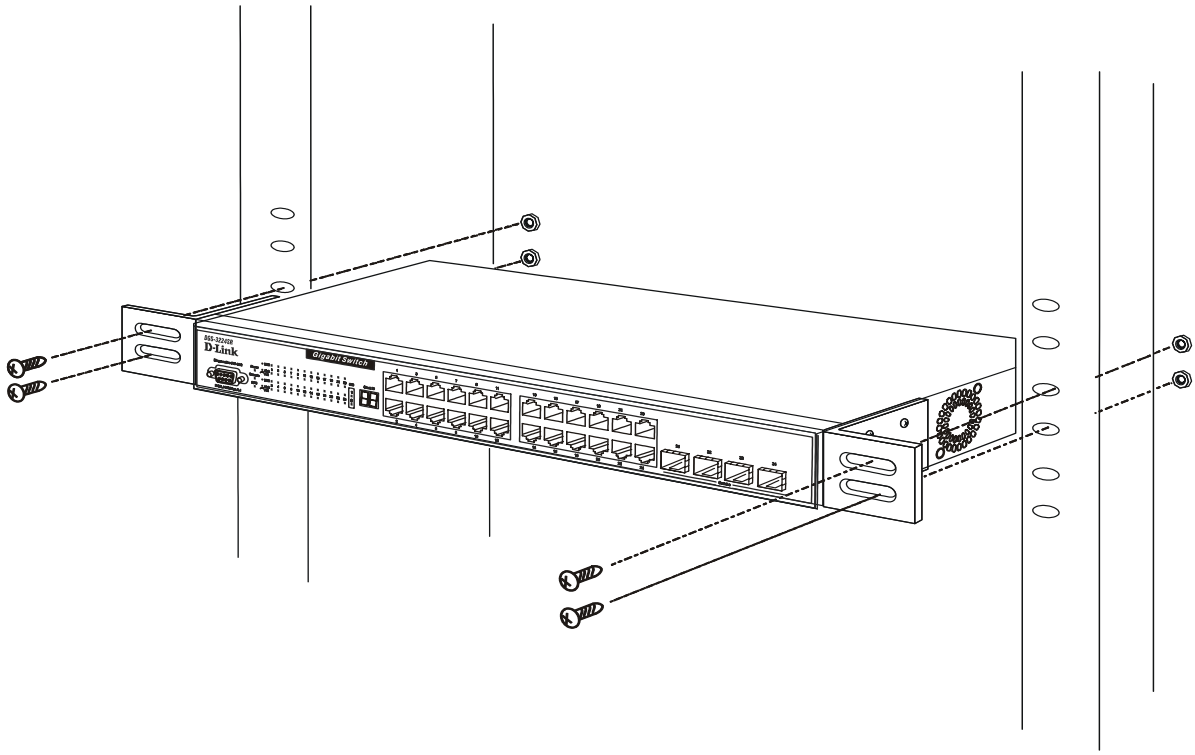


Figure 2-3. Install switch in equipment rack

Connecting Stacked Switch Groups

Up to 12 Switches can be stacked together for Ring mode or Chain mode to a Master Unit or in tandem with a second master unit via the second 10Gig stacking port. Users can add unit to reach maximum 288 GbE ports per Ring stack or 168 GbE ports per Star stack. Switches are stacked together through a high-speed stack cables that provide high speed of multiple Gigabit connections, allowing the entire stack to perform as a single IP entity. User can see the number of switches stacked together from 7-segment display on front panel. Please refer to the diagram below.

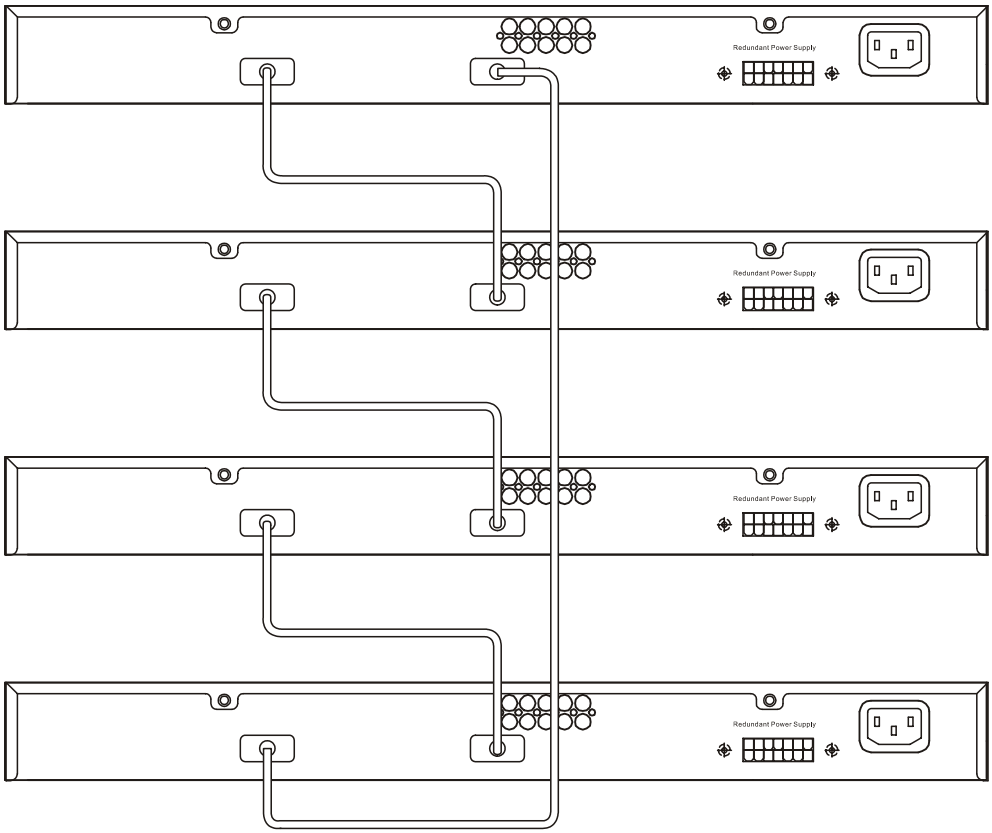


Figure 2-4. Ring (Bus) Topology

Please note that the **DGS-3324SRi** is needed to connect a group of Switches in the Star topology, as shown below.

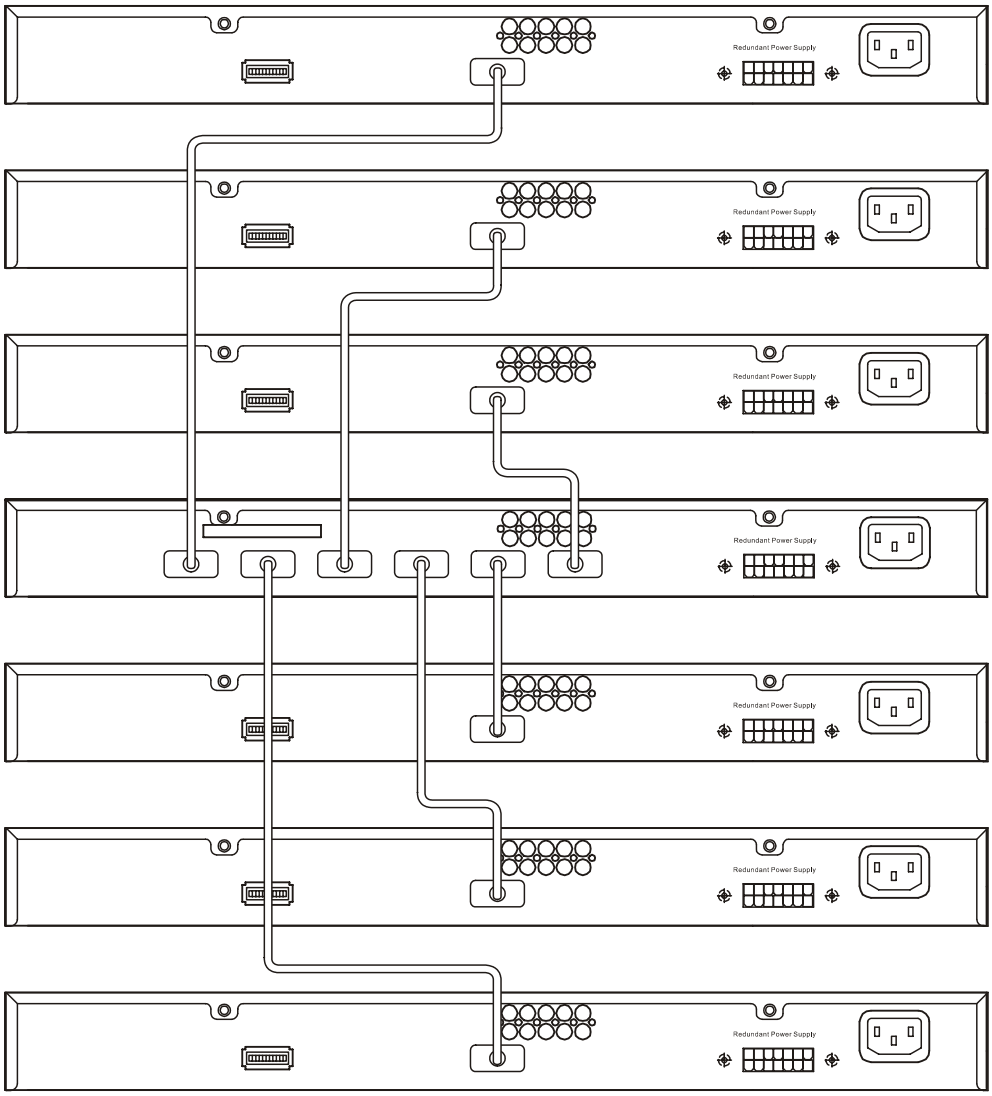


Figure 2-5. Star Topology Stacked Switch Group

The stacking ports are designated 1 and 2, and the stacking port being used will have its matching LED (on the front panel) light a steady green when in use. Connection can be made from any stacking port to any other stacking port. That is, stacking port 1 may connect to 1 or 2, and stacking port 2 may connect to 2 or 1

Configuring a Switch Group for Stacking

Follow the instructions below to configure the DGS-3224SR as the designated Master, and then to configure the slave units.

To configure the DES-3224SR to function in a stacked group as a master, do the following:

1. At the CLI login prompt, enter **`config box_priority current_box_id 1 priority 1`** and press the Enter key. (Where the lowest priority number in a stack is always the Master, i.e. 2 would have a higher priority than 5.)
2. Successful configuration will be verified by a **Success** message. It takes a few seconds for the change to take effect. See the example below for the DES-3224SR.
3. Be sure to save the configuration change using the CLI command **`save`**.
4. Reboot the Switch.

```
DGS-3223Sr:4#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

 Success.

DES-3224SR:4#.....
DES-3224SR:4#
```

To configure the same DGS-3224SR to function in a stacked group as the Slave, do the following:

1. At the CLI login prompt, enter **`config box_priority current_box_id 1 priority 2`** and press the Enter key.
2. Successful configuration will be verified by a **Success** message. It takes a few seconds for the change to take effect. See the example below for the DGS-3224SR.
3. Be sure to save the configuration change using the CLI command **`save`**.

```
DGS-3224SR:4#config box_priority current_box_id 1 priority 2
Command: config config box_priority current_box_id 1 priority 2

 Success.

DGS-3224SR:4#.....
```

Note: Make sure that each box has a different ID. No two boxes can have the same ID.

Unit ID Display for Switches in a Switch Stack

The **Stack ID**. 7-segment LED (as shown below) on the front panel displays the Stack ID of the Switch. Please also note that the **Master** LED is lit, indicating that this Switch is the Master unit in the stack.

Gigabit Combo Ports

In addition to the 24 10/100/1000 Mbps ports, the Switch features four Mini-GBIC Combo ports. These four ports are 10/100/1000BASE-T copper ports (built-in) and Mini-GBIC ports (optional). Please note that the Mini-GBIC ports are used instead of the built-in 10/100/1000BASE-T ports. The Mini-GBIC ports will not work simultaneously with its corresponding 10/100/1000BASE-T port. For example, if port 24x is used on the Mini GBIC module, port 24 is not available for the 10/100/1000BASE-T built-in port, and vice versa.

External Redundant Power System

The switch supports an external redundant power system.

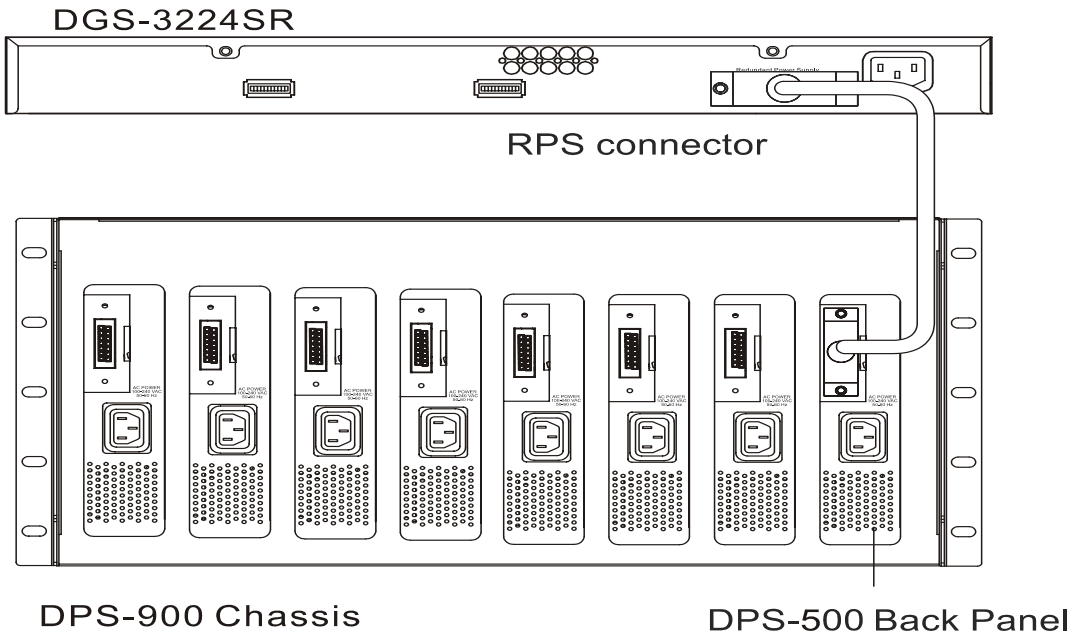


Figure 2-6. DPS-500 with DES-3224SR

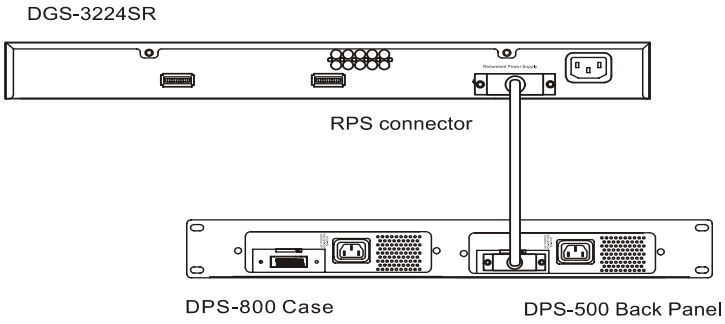


Figure 2-7. DPS-800 with DES-3224SR

NOTE: See the DPS-500 documentation for more information.

CAUTION: Do not use the switch with any redundant power system other than the DPS-500.

Connecting the Console Port

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 DB-9 connector, implemented as a DCE 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 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 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 115200 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 *Command Line Reference* on the documentation CD for a list of all commands and additional information on using the CLI.
12. When you have completed your tasks, exit the session with the **logout** command or close the emulator program.

Password Protection

The DGS-3224SR 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".

```
DGS-3224SR:4#create account admin newmanager
Command: create account admin newmanager

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

DGS-3212SR: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) function 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 DGS-3224SR supports the SNMP versions 1, 2c, and 3. You can specify which version of the 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 next section, 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 from the initial boot console screen – shown below.

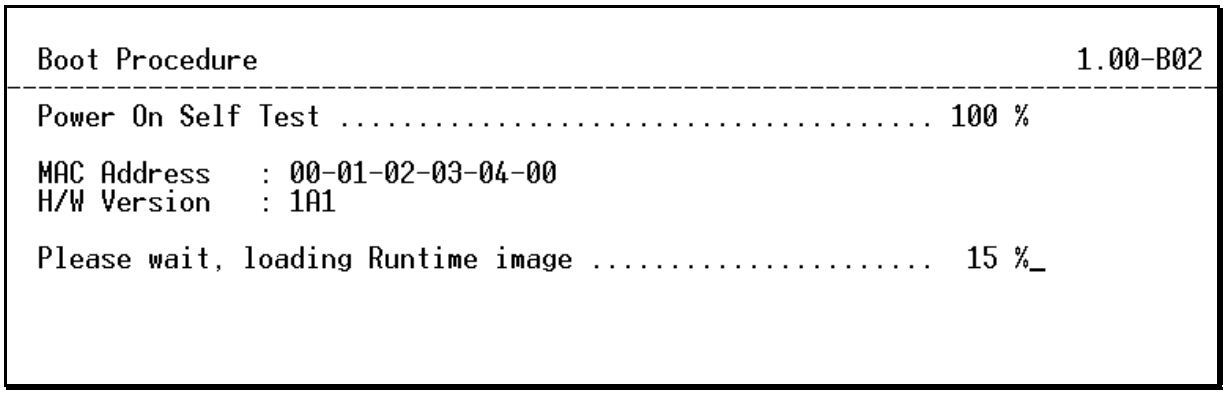


Figure 2 - 4. Boot Screen

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.

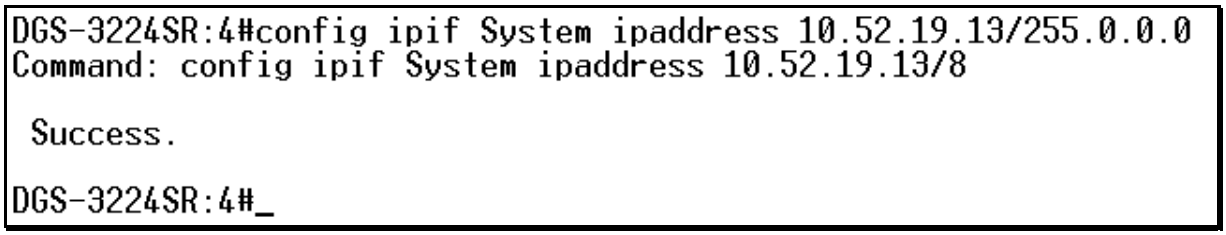


Figure 2 - 5. Assigning the Switch an IP Address

In the above example, the switch was assigned an IP address of 10.52.19.13 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 3

Introduction to Switch Management

Login to Web Manager

Web-based User Interface

Basic Setup

Switch Information

IP Address

User Accounts

Saving Changes

Factory Reset

Restart System

Introduction

All software functions of the DGS-3224SR 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 at the top of the window:

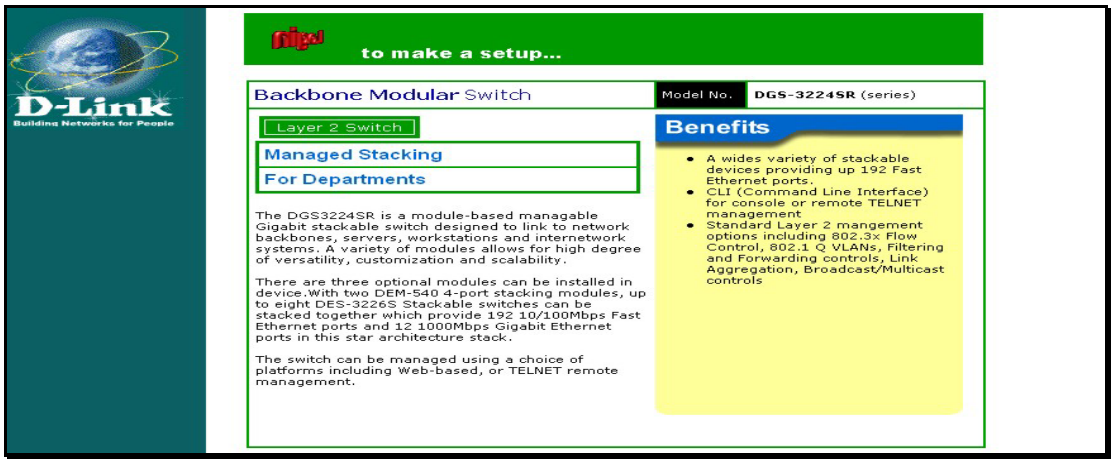


Figure 3-1. Login Page

This opens the management module's main page.

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.

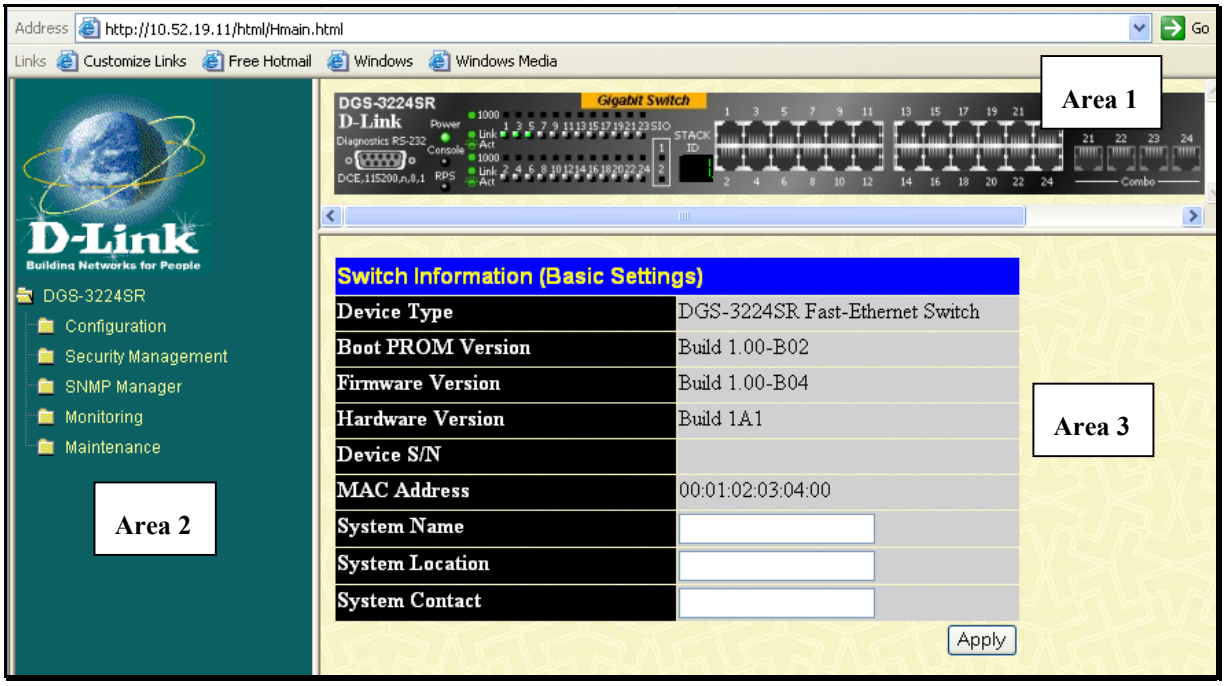


Figure 3-2. Main Web-Manager Screen

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:

Configuration folder: includes menus for port configuration, bandwidth control, link aggregation, port mirroring, VLANs configuration, Spanning Tree Protocol setup, forwarding & filtering configuration, Quality of Service, broadcast/multicast storm controls (Traffic Control), IGMP snooping, static router ports setup, SysLog server setup, port security, SNTP settings and the access profile table. This also contains the Advanced Settings menu which is used to configure miscellaneous settings such as for the serial port, MAC address aging time, and to enable/disable the following: RMON, IGMP snooping, Telnet and web management access, traffic segmentation, and 802.1x. The Switch Information page is used to enter system contact and physical location information and lists basic information such as the switch's MAC address, current firmware version and the modules installed.

Security Management: contains 802.1x settings including Radius server information and PAE setup and security management IP station setup.

SNMP Manager: contains menus for establishing the switch IP settings, user accounts configuration and SNMP setup including SNMP v.3 configuration.

Monitoring: includes menus for monitoring switch performance monitors, MAC address table information, router port information, IGMP Snooping information and 802.1x related information.

Maintenance: contains menus for upgrading firmware and saving configuration files (TFTP Services), saving configuration changes, resetting and rebooting the switch, Ping test and logging out of the web manager.

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.

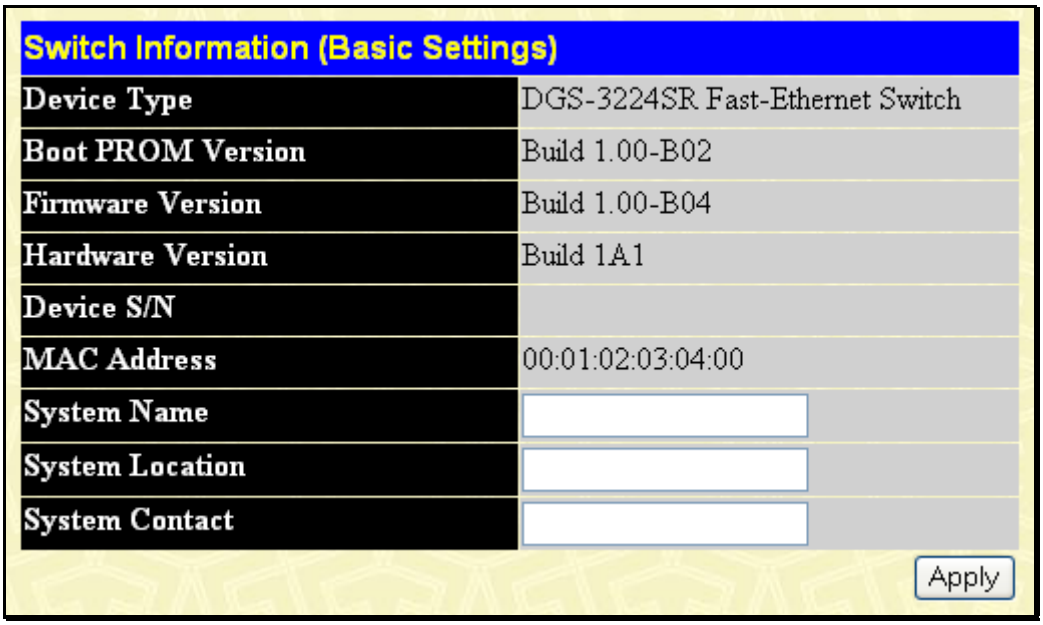


Figure 3-3. Switch Information – Basic Settings

The **Switch Information** window shows the switch's **MAC Address** (assigned by the factory and unchangeable). 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.

You may assign a System Name, System Location, and System Contact. If any changes or additions are made, click **Apply**.

Switch IP Settings

Switch IP settings 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 **IP Address** menu located in the **Configuration** folder.

To configure the switch's IP address:

Open the **Configuration** folder and click the **IP Address** menu button. The web manager will display the **Switch IP Settings** menu below.

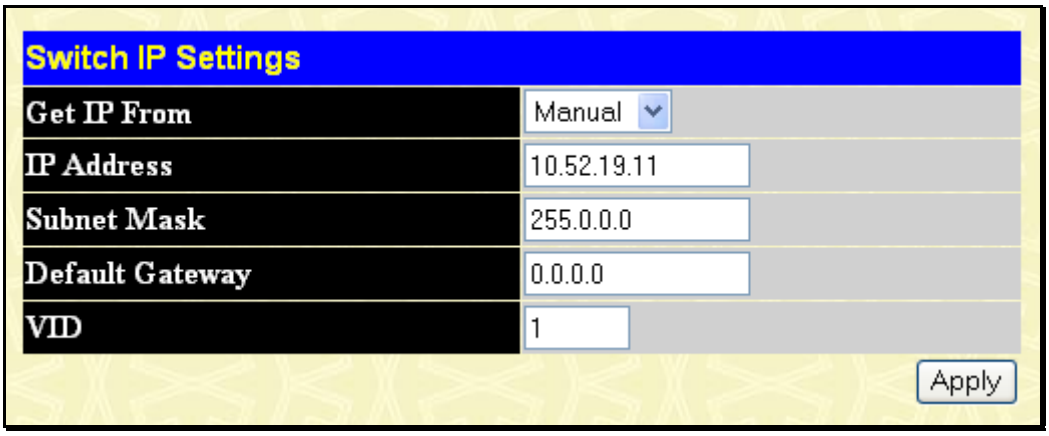


Figure 3-4. Configure Switch IP Settings

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 ID (VID) 1. 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 Switch IP Settings 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 (see page 31) is specified or Management Station IP Addresses (see page 20) 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.

Security IP Management Stations Configuration

Go to the **Security Management** folder and click on **Security IP**; the following screen will appear.

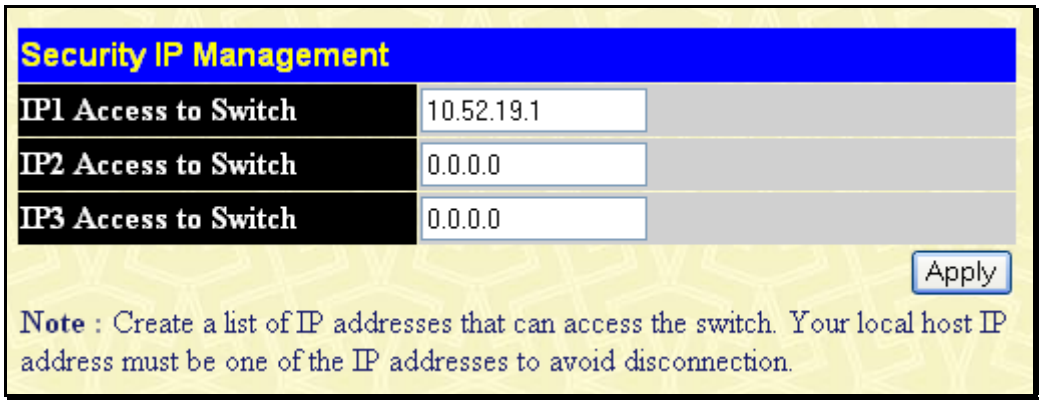


Figure 3-5. Security IP Management Setup

Use the Management Station IP Settings to select up to three management stations used to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address and click on the **Apply** button.

User Accounts Management

Use the User Accounts Control Table to control user privileges. To view existing User Accounts, open the **Security Management** folder and click on the **User Accounts** link. This will open the **User Account Management** page, as shown below.

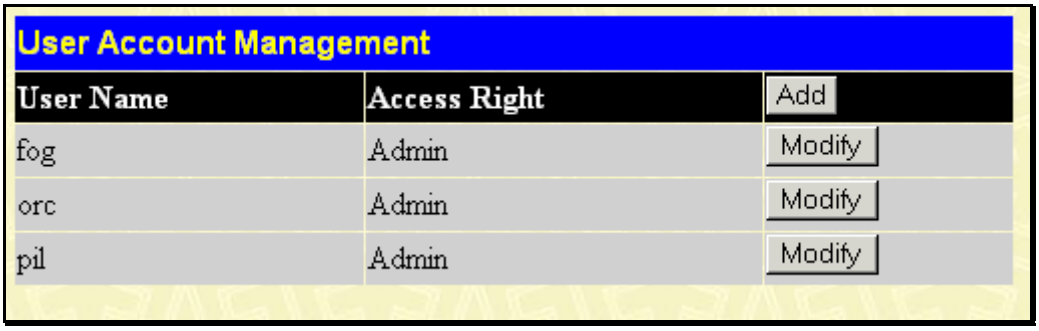


Figure 3-6. User Accounts Management Table

To add a new user, click on the **Add** button. To modify or delete an existing user, click on the **Modify** button for that user.

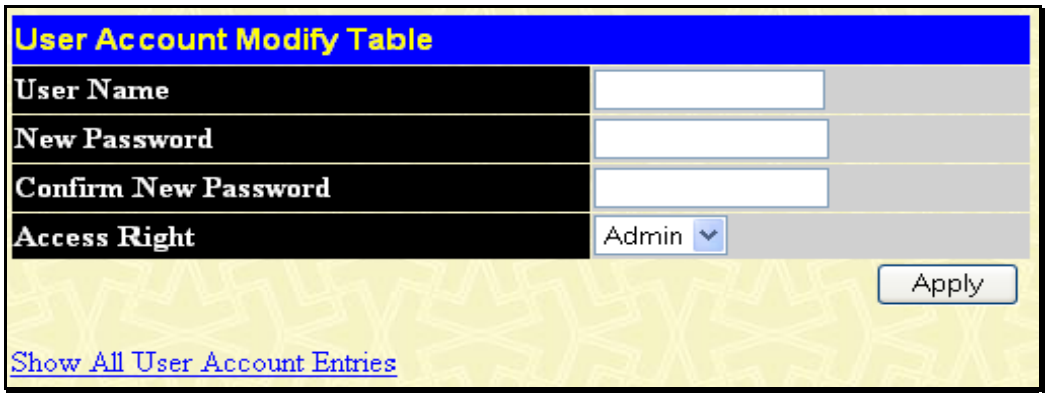


Figure 3-7. Add User Accounts Modify Table

Add a new user by typing in a **User Name**, and **New Password** and retype the same password in the **Confirm New Password**. Choose the level of privilege (**Admin** or **User**) from the **Access Right** drop-down menu. To add a user account using the CLI commands use **create account** and **config account**.

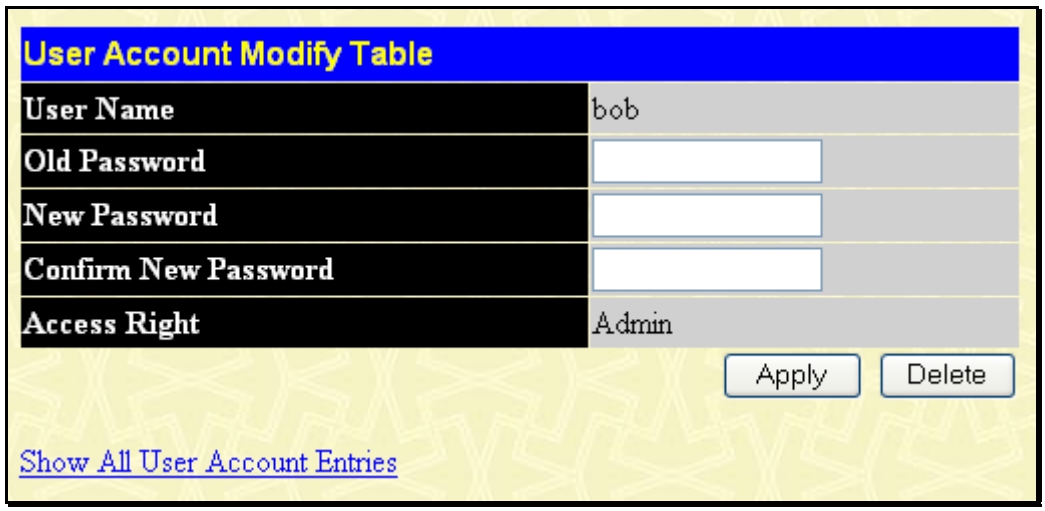


Figure 3-8. Modify User Accounts

Modify or delete an existing user account in the User Account Control Table – Edit. To delete the user account, click on the **Delete** button. To change the password, type in the **New Password** and retype it in the **Confirm New Password** entry field. Choose the level of privilege (**Admin** or **User**) from the **Access Right** drop-down menu. To delete a user account using CLI use the command **delete account**. To change an existing account use **config account**.

From the **Main Menu**, highlight **Setup User Accounts** and press Enter, then the **User Account Management** menu appears.

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:

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	No
System Utilities	Yes	Ping Only
Factory Reset	Yes	No
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

Admin and User Privileges

After establishing a User Account with **Admin**-level privileges, be sure to save the changes (see below).

Saving Changes

Changes made to the switch's configuration must be saved in order to retain them. Access the **Save Configuration** by clicking the **Save Changes** button located in the **Maintenance** folder.

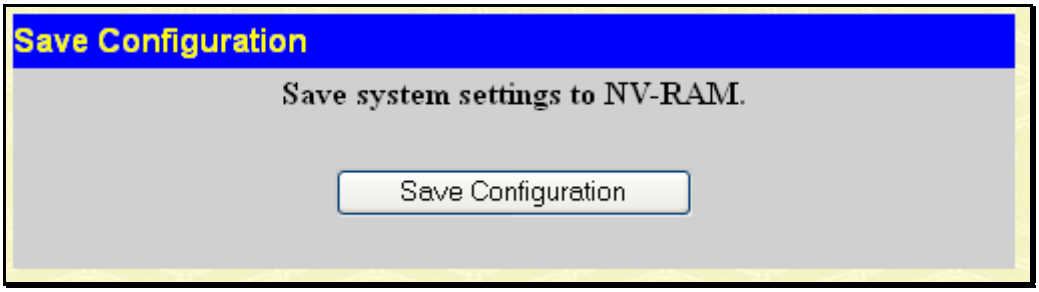


Figure 3-9. Save Configuration window

The switch has two levels of memory, normal RAM and non-volatile or NV-RAM. To save all the changes made in the current session to the Switch's flash memory, click the **Save Configuration** button. Click the **OK** button in the new dialog box that appears to continue. When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect. Once the switch configuration settings have been saved to NV-RAM, they become the default settings for the switch. These settings will be used every time the switch is rebooted.

Some settings, though, require you to restart the switch before they will take effect. Restarting the switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

To save settings using CLI the command is **save**.

Factory Reset

Click the **Factory Reset** link in the **Maintenance** folder to bring up the reset menu.

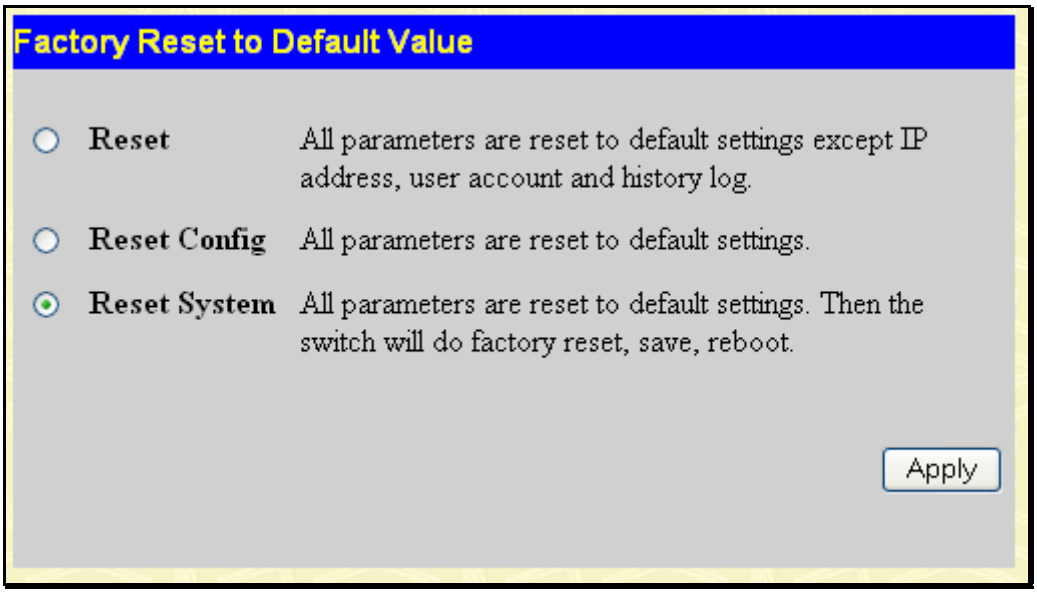


Figure 3-10. Factory Reset to Default Value

Reset – returns all configuration settings except the switch's IP address, subnet mask, default gateway, log, user account and stack information settings to the factory default settings.

Reset Config – returns all configuration settings except the stack information settings to the factory default settings, but does not save the settings or reboot the switch. If you select this option the switch configuration will be returned to the factory default settings for the current session only. When the switch is rebooted, it will return to the last configuration saved to the switch's NV-RAM using the **Save Changes** option.

Reset System – returns switch configuration to the factory default settings and then saves the factory default configuration to the switch's NV-RAM. The switch will then reboot. When the switch has rebooted, it will have the same configuration as when it was delivered from the factory.

Restart System

The following menu is used to restart the switch. Access this menu by clicking on the **Reboot Device** link in the **Maintenance** folder.

Click the **Yes** after **Do you want to save the settings?** to instruct the switch to save the current configuration to non-volatile RAM before restarting the switch.

Clicking the **No** option instructs the switch not to save the current configuration before restarting the switch. All of the configuration information entered since the last time **Save Changes** was executed will be lost.

Click the **Restart** button to restart the switch.

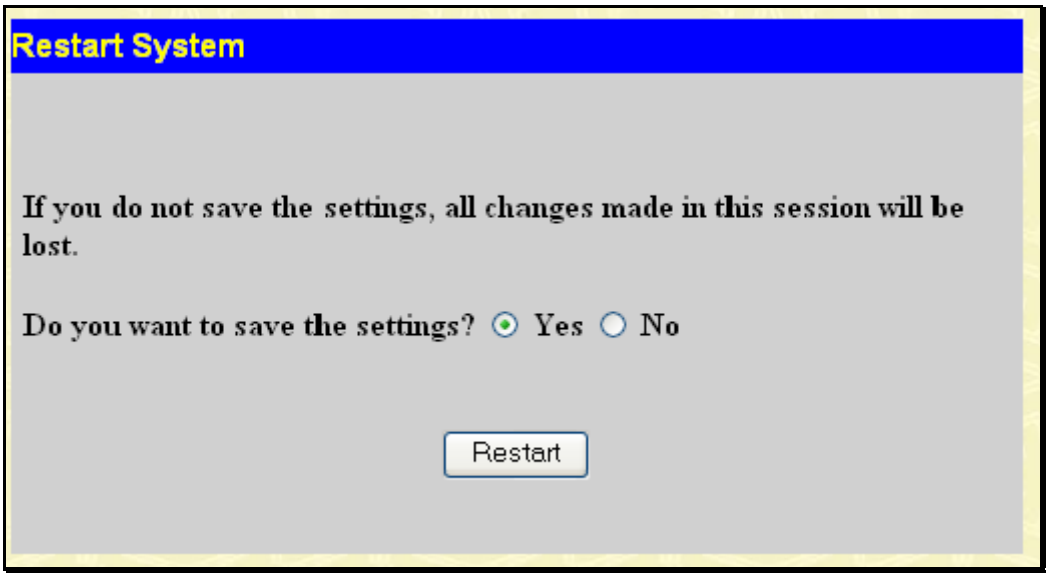


Figure 3-11. Restart System

NOTE: clicking **Yes** is equivalent to executing **Save Changes** and then restarting the switch.

Switch Information

The first page displayed upon logging in presents the **System Information** menu. This page can be accessed at any time by clicking the **Switch Information** button in the **Configuration** folder.

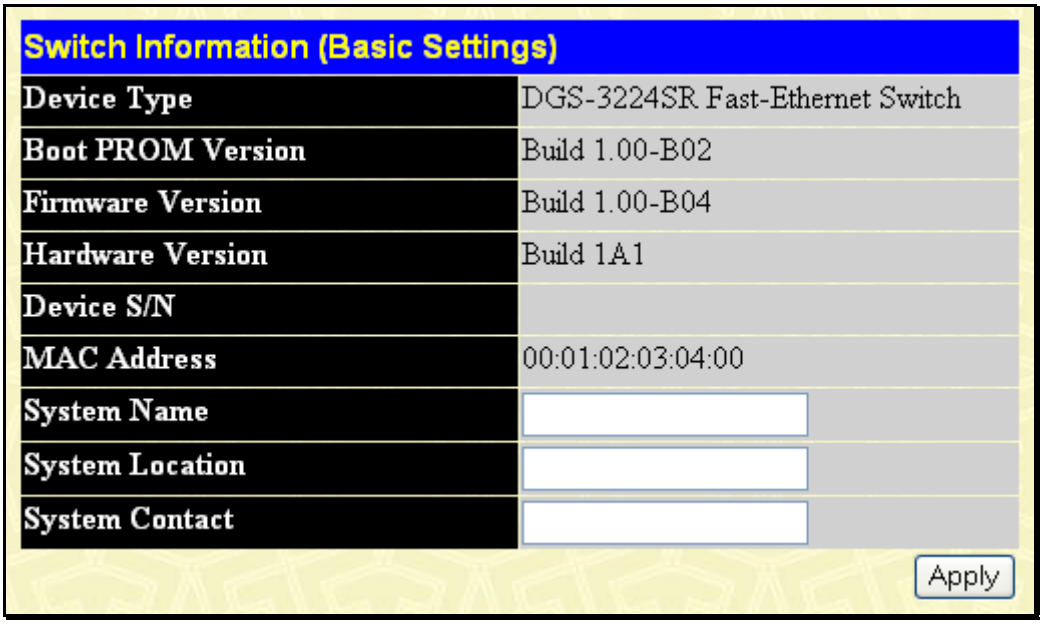


Figure 3-12. Switch Information

The **System Information** page displays general information about the Switch including its MAC Address, Hardware Boot PROM and Firmware versions, and other optional information.

You can also enter or change a **System Name**, **System Location**, and the name and telephone number of the responsible administrator in the **System Contact**. It is recommended that the person responsible for the maintenance of the network system be listed here. Click on the **Apply** button to make the changes effective.

To view this information using Telnet use CLI command **show switch**.

Advanced Settings

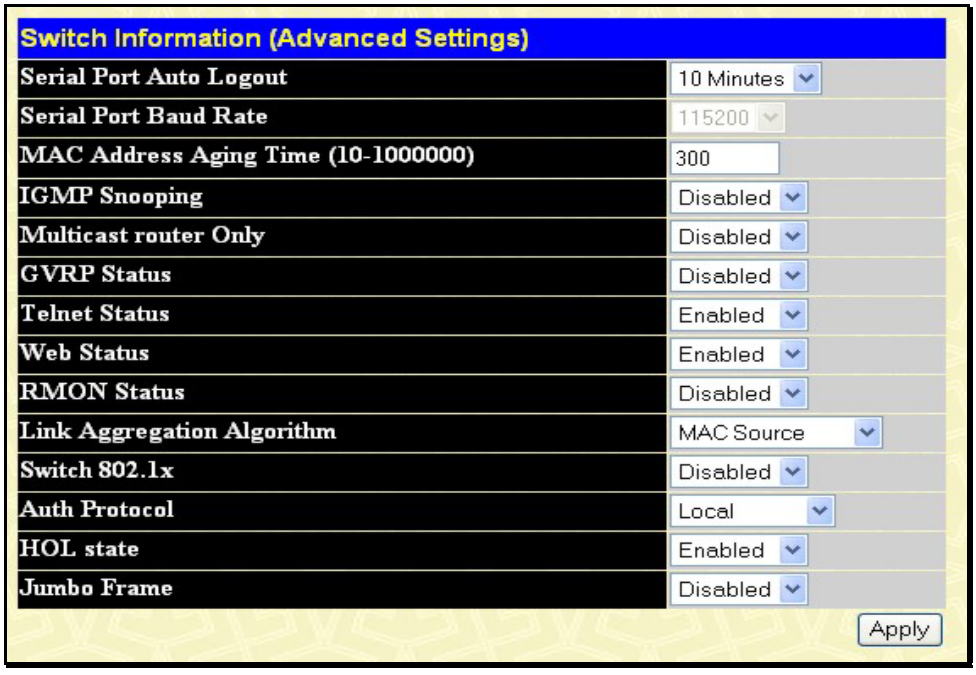


Figure 3-13. Switch Information – Advanced Settings

The Advanced Settings menu options are summarized in the table below.

Variables in the Advanced Settings menu of the Web Manager and their corresponding CLI command groups are the following:

Parameter	Description
Serial Port Auto Logout	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: *2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes* or *Never.*
Serial Port Baud Rate	Fixed at 115200.
MAC Address Aging Time	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 default age-out time for the Switch is 300 seconds. To change this, type in a different value representing the MAC address age-out time in seconds. The Aging Time can be set to any value between **10** and **1,000,000** seconds.
IGMP Snooping	To enable system-wide IGMP Snooping capability select *Enabled*. IGMP snooping is *Disabled* by default. Enabling IGMP snooping allows you to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the **IGMP Snooping** page under the **IGMP** folder.
Multicast Router Only	If this option is enabled and IGMP Snooping is also enabled, the switch forwards all multicast traffic to a multicast-enabled router only. Otherwise, the switch will forward all multicast traffic to any IP router.
Telnet Status	Telnet configuration is *Enabled* by default. If you do not want to allow configuration of the system through Telnet choose *Disabled*.
Web Status	Web-based management is *Enabled* by default. If you choose to disable this by selecting *Disabled*, you will lose the ability to configure the system through the web interface as soon as these settings are applied.
RMON Status	Remote monitoring (RMON) of the switch is *Enabled* or *Disabled* here.
GVRP	Use this pull-down menu to **Enable** or **Disable** GVRP on the switch.
Link Aggregation Algorithm	The algorithm that the switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose *Source Address, Destination Address* or *Both.* (See Link Aggregation).
Switch 802.1x	Enables or disables 802.1x VLANs; default is Disabled.
Auth Protocol	Fixed at Radius Eap.
HOL Prevention State	Enables or disables HOL (Head of Line) prevention; default is Enabled.
Jumbo Frame	Enables or disables Jumbo Frame acceptance; default is Disabled.
Syslog State	Enables or disables Syslog State; default is Disabled.

Section 4

Switch Stack Management

The DGS-3224SR switch can be used as a standalone high-capacity switch or be used in a stacked arrangement.

One stacking module can be installed to stack up to 4 additional slave switch units or two modules can be installed to stack up to 8 additional slave switch units. Please read the relevant information in Sections 1 and 2 for more information.

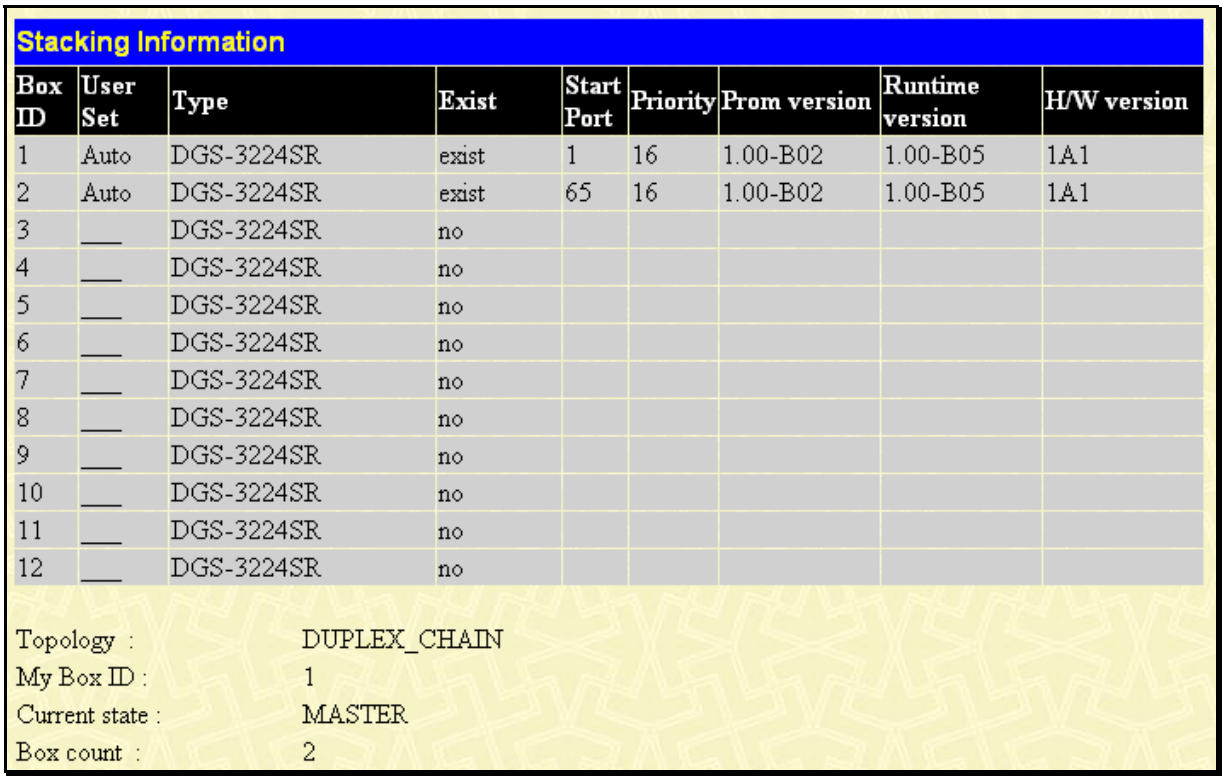
Stacking Information

To change a switch's default stacking configuration (for example, the order in the stack), you must use the console Command Line Interface.

The number of switches in the switch stack (up to 12 – total) are displayed in the upper right-hand corner of your web-browser. The icons are in the same order as their respective Unit numbers, with the Unit 1 switch corresponding to the icon in the upper left-most corner of the icon group.

When the switches are properly interconnected through their optional Stacking Modules, information about the resulting switch stack is displayed under the **Stack Information** link.

To view the stacking information, click on the Stacking Information link from the Monitoring folder:



Stacking Information

Box ID	User Set	Type	Exist	Start Port	Priority	Prom version	Runtime version	H/W version
1	Auto	DGS-3224SR	exist	1	16	1.00-B02	1.00-B05	1A1
2	Auto	DGS-3224SR	exist	65	16	1.00-B02	1.00-B05	1A1
3	___	DGS-3224SR	no					
4	___	DGS-3224SR	no					
5	___	DGS-3224SR	no					
6	___	DGS-3224SR	no					
7	___	DGS-3224SR	no					
8	___	DGS-3224SR	no					
9	___	DGS-3224SR	no					
10	___	DGS-3224SR	no					
11	___	DGS-3224SR	no					
12	___	DGS-3224SR	no					

Topology : DUPLEX_CHAIN
My Box ID : 1
Current state : MASTER
Box count : 2

Figure 4-1. Stacking Information

Box ID – displays the switch's order in the stack.

Type – displays the model name of the corresponding switch in a stack.

User Set – Box ID can be assigned automatically (Auto), or can be assigned statically. Default is Auto.

Exist – Denotes whether a switch does or does not exist in a stack**.**

Priority – Displays the priority ID of the Switch. The lower the number, the higher the priority. The box (switch) with the lowest priority number in the stack is the Master switch.

PROM Version – Shows the PROM in use for the Switch. This may be different from the values shown in the illustration.

H/W Version – Shows the hardware version in use for the Switch. This may be different from the values shown in the ullustration.

Runtime Version – Shows the firmware version in use for the Switch. This may be different from the values shown in the illustrations.

The switch's current order in the switch stack is also displayed on the front panel, under the **STACK NO.** heading.

Alternatively, the stacking order can be manually assigned using the console's Command Line Interface (CLI).

You can use the **show stack_information** command to display the current switch stack information. The syntax of the **show stack_information** command is as follows:

show stack_information

Using the optional parameter **mode** displays only the stacking mode of the switches in the switch stack.

Entering the **show stack_information** command returns all of the relevant stacking information for all of the switches in the stack:

```
Command: show stack_information

 Box User                    Start Prio- Prom     Runtime   H/W
 ID  Set  Type        Exist  Port  rity  version  version   version
 --- ---- ----------- ----- ----- ----- -------- -------- --------
   1 AUTO DGS-3224SR  exist     1    16 1.00-B02 1.00-B05 1A1
   2 AUTO DGS-3224SR  exist    65    16 1.00-B02 1.00-B05 1A1
   3 ____ DGS-3224SR  no
   4 ____ DGS-3224SR  no
   5 ____ DGS-3224SR  no
   6 ____ DGS-3224SR  no
   7 ____ DGS-3224SR  no
   8 ____ DGS-3224SR  no
   9 ____ DGS-3224SR  no
  10 ____ DGS-3224SR  no
  11 ____ DGS-3224SR  no
  12 ____ DGS-3224SR  no
 ------------------------------------------------------------------
Topology     :DUPLEX_CHAIN
My Box ID    :1
Current state:MASTER
Box Count    :2

DGS-3224SR:4#
```

Figure 4-2. Console CLI show stack_information command

The same switch stack information is displayed in the console as is displayed in the Web-based management agent.

To modify the box ID, use the **config box_id** command, first identifying the current box ID and then assigning a new box ID, as follows:

```
DGS-3224SR:4#config box_id current_box_id 11 new_box_id 5
Command: config box_id current_box_id 11 new_box_id 5

 Success.

DGS-3224SR:4#
```

Use the following command to modify all box_id to become AUTO or static (apply current box id to User Set), use the following syntax:

Config all_box_id [auto_mode|static_mode]

The **config box_priority** command allows you to configure the switch stack manually.

The syntax of the **config box_priority** command is as follows:

config box_priority current_box_id <1-12> priority <1-16>

Where the highest priority is assigned to the lowest value, i.e. 2 is a higher priority than 5.

Note: Box-priority settings will take effect after the switch is rebooted.

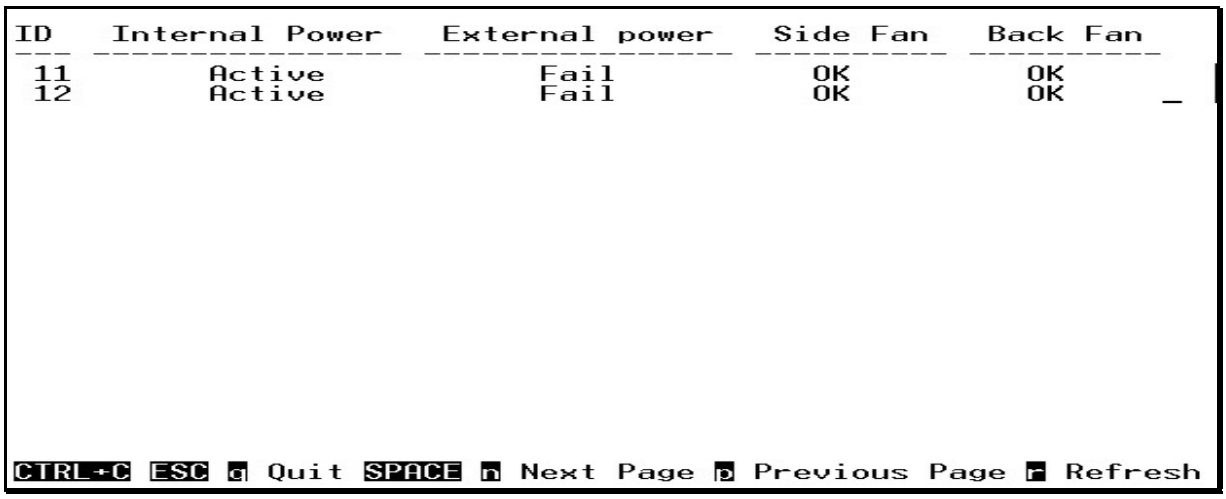
```
DGS-3224SR:4#
DGS-3224SR:4#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

 Success.

DGS-3224SR:4#
```

Figure 4-3. Config box_priority Command

You can then use the **show stack_information** command. Or, to see the status of only existing switches, use the command **show device_status.** The resulting screen shows the status of internal and external power systems and also shows the status of the cooling fans on each device. Click on **Esc** to return to the CLI screen.


ID Internal Power External power Side Fan Back Fan
11 Active Fail OK OK
12 Active Fail OK OK
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh

Section 5

VLAN Configuration

The first half of this section describes how to use the web manager to configure VLANs in the switch. This is followed by a review of some of the basic concepts of VLANs in an Ethernet switching environment. For a detailed list of CLI commands associated with VLAN management, please read the CLI reference guide.

To create or modify an 802.1Q VLAN:

In the **Configuration** folder, open the **VLAN** folder and click the **Static VLAN Entry** link to open the following window:

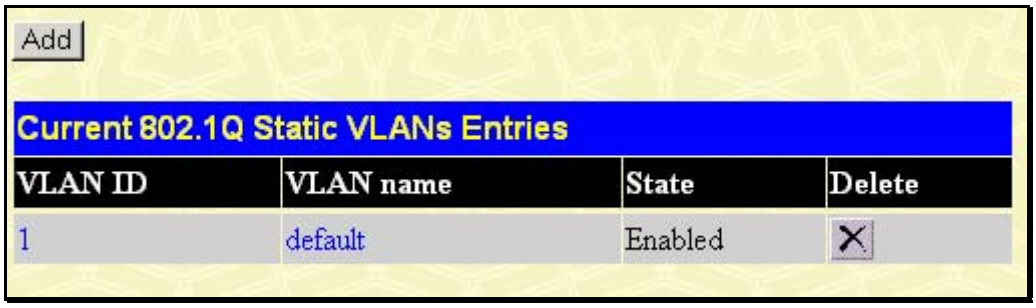


Figure 5-1. 802.1Q Static VLANs

The 802.1Q Static VLANs menu lists all previously configured VLANs by VLAN ID and name. To delete an existing 802.1Q VLAN, click the corresponding **Delete** button.

To create a new 802.1Q VLAN, click the **Add** button in the Static VLANs menu. A new menu appears, use this to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.

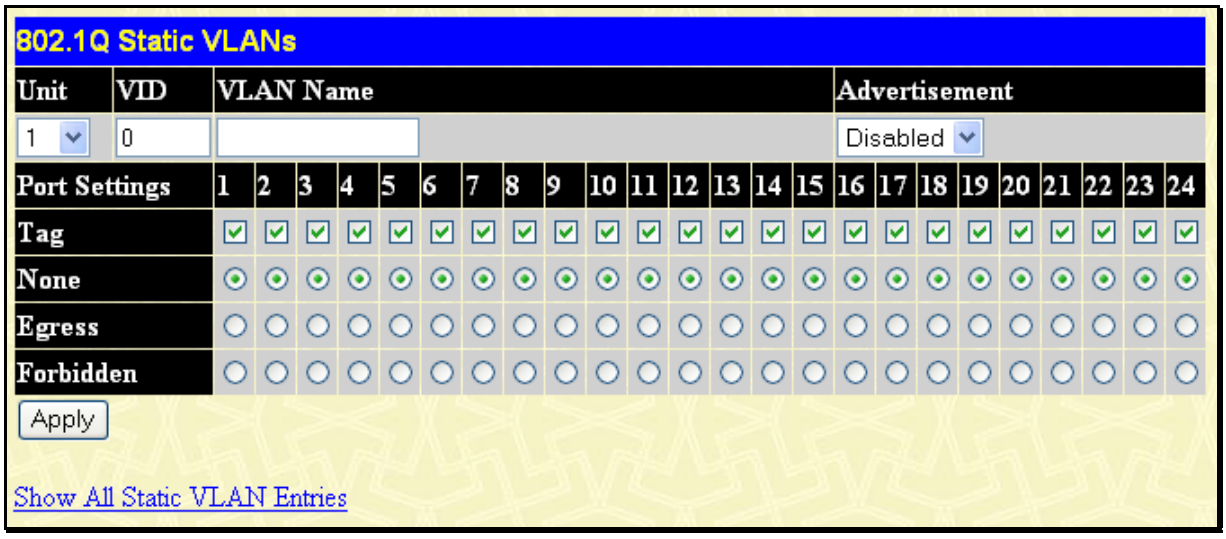


Figure 5-2. 802.1Q Static VLANs Entry Settings – Add

To change an existing 802.1Q VLAN entry, double-click on the selected entry in the 802.1Q Static VLANs menu. A new menu appears, use this to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.

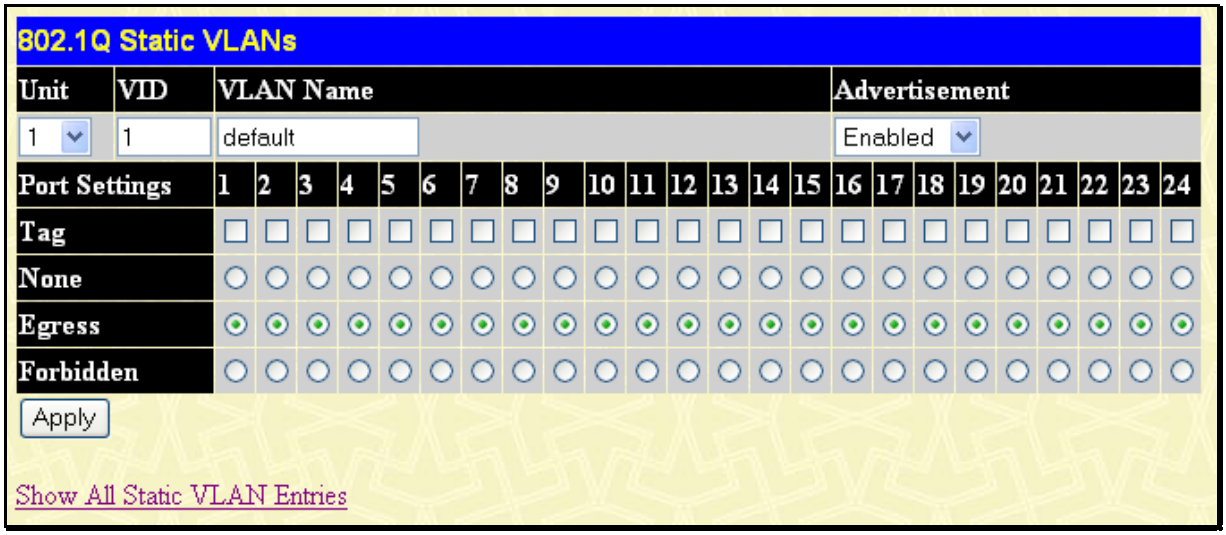


Figure 5-3. 802.1Q Static VLANs Entry Settings – Modify

The following fields can then be set in either the **Add** or **Modify** 802.1Q Static VLANs menus:

Parameter	Description
VID (VLAN ID)	Allows the entry of a VLAN ID in the Add dialog box, or displays the VLAN ID of an existing VLAN in the Edit dialog box. 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 dialog box, or for editing the VLAN name in the Edit dialog box.
Port	Allows an individual port to be specified as member of a VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
Egress	Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

GVRP Setting

In the **Configuration** menu, open the **VLANs** folder and click **GVRP Setting**.

The **Port VLAN ID (PVID)** dialog box, shown below, allows you to determine whether the switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (**GVRP**) enabled switches. In addition, **Ingress Checking** can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port.

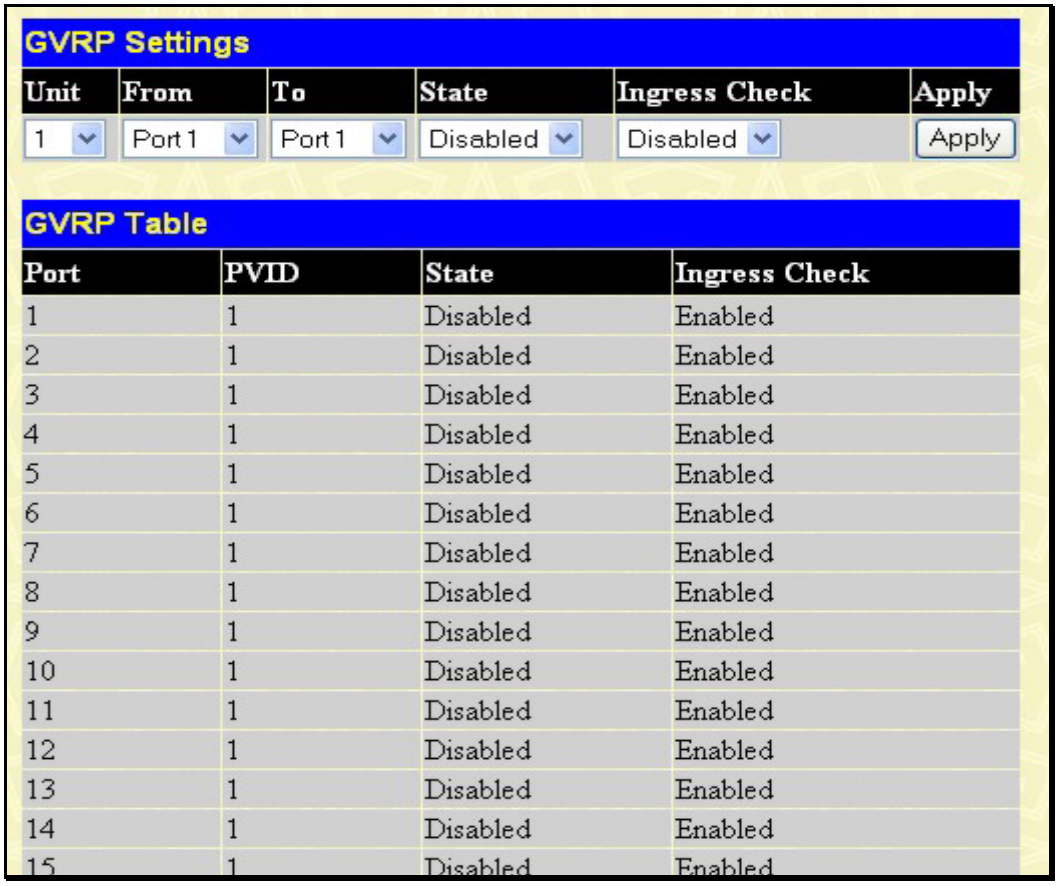


Figure 5-4. GVRP Setting

The following fields can be set:

Parameter	Description
Unit	Displays the Unit ID of the switch – within the switch stack – that the VLAN will be created on.
From/To	These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **802.1Q Port Settings** page.
PVID	A Port VLAN Identifier is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the Edit 802.1Q VLANs menu above.
GVRP State	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is disabled by default.
Ingress Check	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables Ingress filtering. Ingress Checking is disabled by default.

Configure 802.1Q Static VLANs

The following figures and tables describe how to set up static VLANs on the switch. Click on the **Static VLAN Entry** link in the **VLANs** folder to open the **802.1Q Static VLANs** page, as shown below.

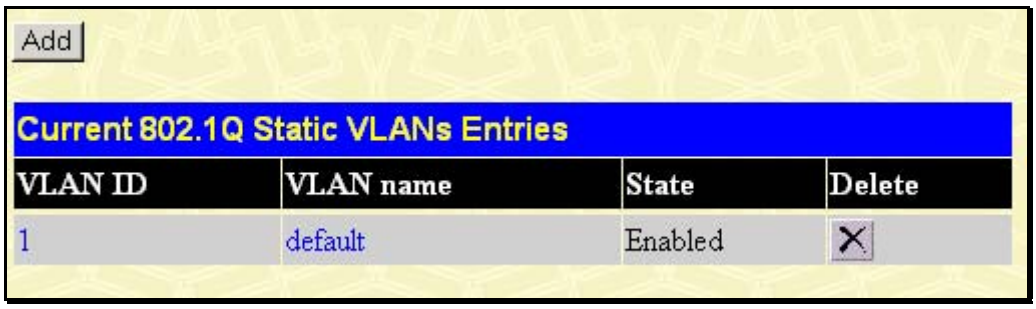


Figure 5-5. 802.1Q Static VLANs Page

The Static VLANs menu lists existing VLANs by their VLAN ID (VID) and by name. To create a new VLAN, click the **Add** button to the upper left of the table. To edit an existing VLAN, double-click on the VLAN you want to edit. To eliminate an entire VLAN, click on the "*X*" button for the VLAN you wish to delete.

The user configurable settings are the same when you Add or Modify a VLAN. Read the next section for a description of these settings.

Add a Static 802.1Q VLAN

The following figure and table describe the parameters that must be configured to add an 802.1Q VLAN on the switch. Click the **Show All Static VLAN Entries** link to return to the **802.1Q Static VLAN** Entries table.

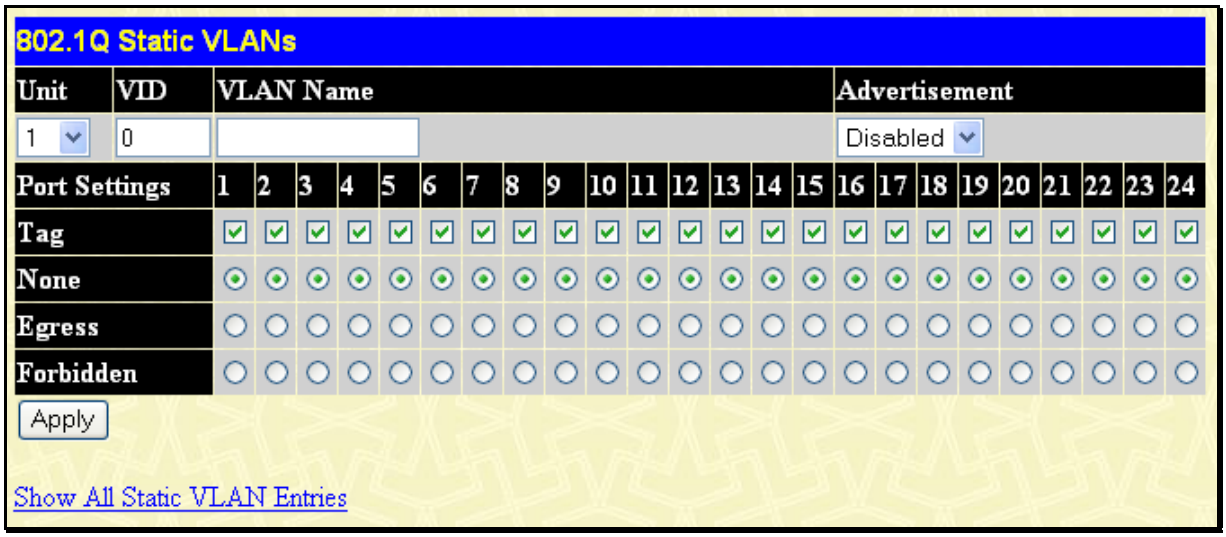


Figure 5- 6. 802.1Q Static VLANs Entry Settings – Add Screen

Parameter	Description
Unit	Displays the Unit ID of the switch – within the switch stack – that the VLAN will be created on.
VID (VLAN ID)	The VLAN ID of the VLAN that is being created.
VLAN Name	The name of the VLAN that is being created.

Port	Corresponds to the ports that will be members of the VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
None	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
Egress	Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.

Edit 802.1Q VLANs

The following figure and table describe how to edit an existing 802.1Q VLAN entry on the switch.

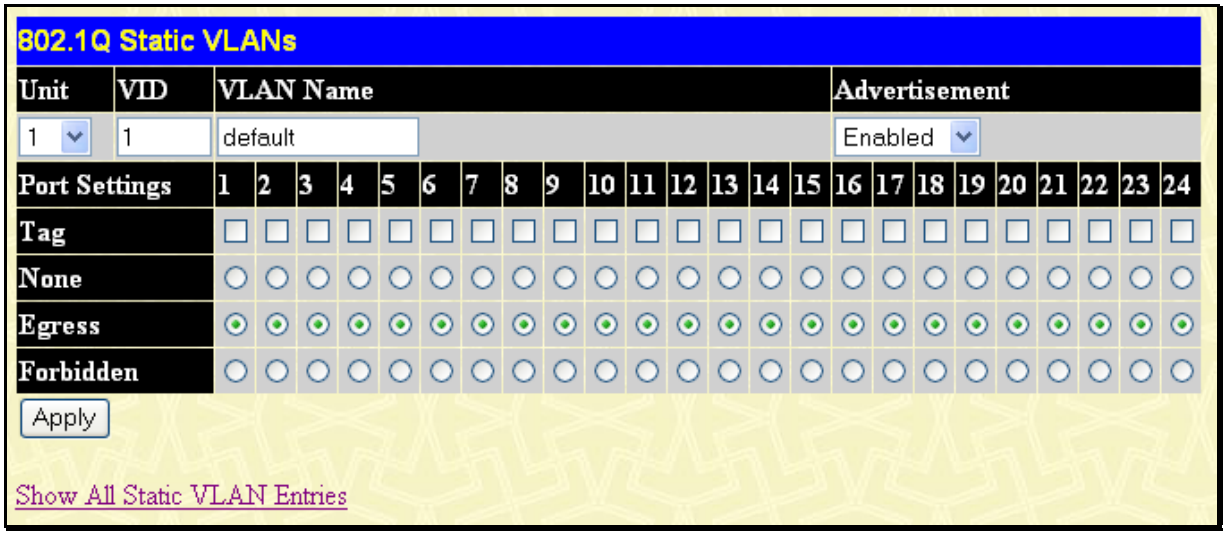


Figure 5-7. 802.1Q Static VLANs Entry Settings – Edit Screen

The Static VLANs Edit screen presents the current configuration of the VLAN. Use this screen to change settings for the VLAN as described in the table below. Click the Show All Static VLAN Entries hyperlink to return to the Current VLAN Entries table.

Parameter	Description
Unit	Displays the Unit ID of the switch – within the switch stack – that the VLAN will be created on.
VID (VLAN ID)	The VLAN ID of the VLAN that is being created.
VLAN Name	The name of the VLAN that is being created.
Port	Corresponds to the ports that will be members of the VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.

None	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
Egress	Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.

Click the **Apply** button to let your changes take effect.

GVRP Settings

Select **VLANs** in the **Configuration** folder, then open **GVRP Settings** and select the Unit and range of ports to configure. For the selected port or group of ports, choose to enable or disable Ingress checking and establish an acceptable packet rule.

The following figure and table describe how to configure the 802.1Q VLAN port settings for the switch.

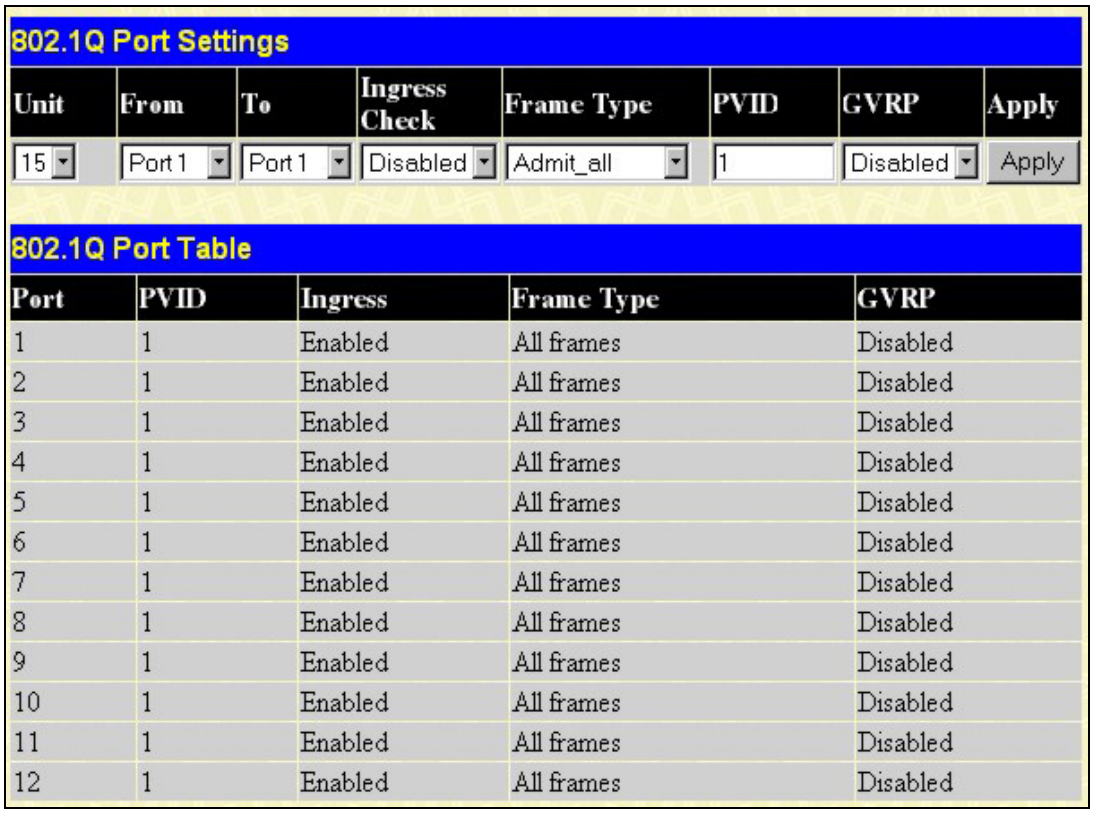


Figure 5-8. GVRP Settings Screen

Click **Apply** to let your changes take effect.

Parameter	Description
Unit	Displays the Unit ID of the switch – within the switch stack – that the VLAN will be created on.
From/To	These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **802.1Q**

	included in the Port-based VLAN that you are creating using the **802.1Q Port Settings** page.
Ingress Check	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables Ingress filtering. Ingress Checking is disabled by default.
PVID	Shows the current PVID assignment for each port. The switch's default is to assign all ports to the Default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames – as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is disabled by default.

Understanding VLANs

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

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 DES-3224SR switch. 802.1Q VLANs require tagging, which enables the VLANs to span an entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

Any port can be configured as either *tagging* or *untagging*. The *untagging* feature of IEEE 802.1Q VLANs allow 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 VLAN compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

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 filter or forward the packet
- Egress rules – determines if the packet must be sent tagged or untagged.

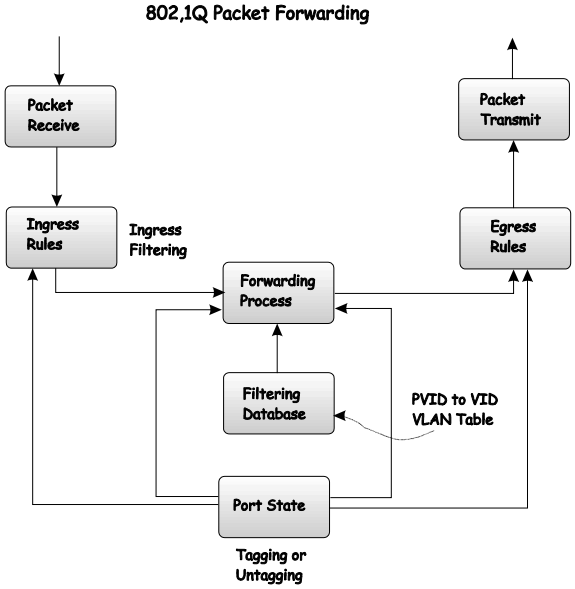


Figure 5-9. IEEE 802.1Q Packet Forwarding

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 or 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 contained in the packet originally is retained.

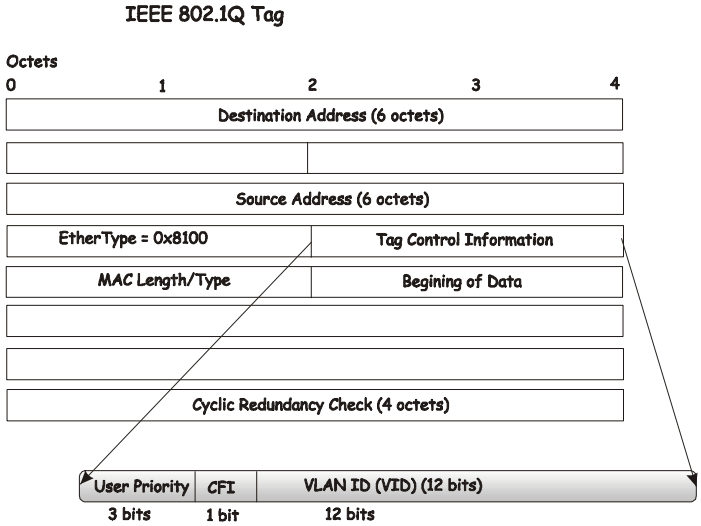


Figure 5-10. IEEE 802.1Q Tag

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.

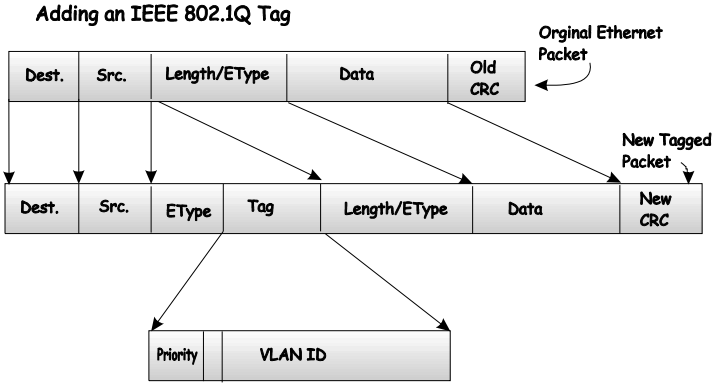


Figure 5-11. Adding an IEEE 802.1Q Tag

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, insofar 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.

Section 6

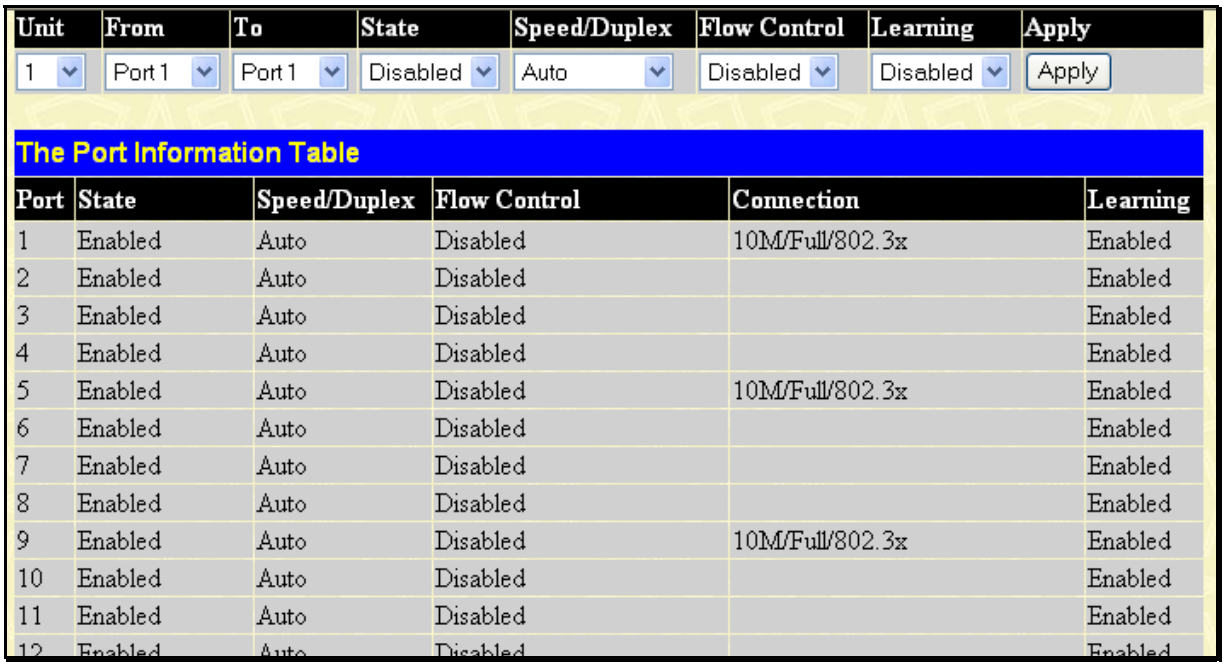
Port Settings Configuration

This section contains information for configuring various attributes and properties for individual physical ports, including port security, traffic segmentation, port bandwidth control, serial port settings and port mirroring.

Basic Port Configuration

To configure basic port settings such as port speed, duplex and learning state use the **Port Configuration** menu.

Click the **Port Configuration** link in the **Configuration** folder:



Unit	From	To	State	Speed/Duplex	Flow Control	Learning	Apply
1	Port 1	Port 1	Disabled	Auto	Disabled	Disabled	Apply

The Port Information Table

Port	State	Speed/Duplex	Flow Control	Connection	Learning
1	Enabled	Auto	Disabled	10M/Full/802.3x	Enabled
2	Enabled	Auto	Disabled		Enabled
3	Enabled	Auto	Disabled		Enabled
4	Enabled	Auto	Disabled		Enabled
5	Enabled	Auto	Disabled	10M/Full/802.3x	Enabled
6	Enabled	Auto	Disabled		Enabled
7	Enabled	Auto	Disabled		Enabled
8	Enabled	Auto	Disabled		Enabled
9	Enabled	Auto	Disabled	10M/Full/802.3x	Enabled
10	Enabled	Auto	Disabled		Enabled
11	Enabled	Auto	Disabled		Enabled
12	Enabled	Auto	Disabled		Enabled

Figure 6-1. Port Configuration

To configure switch ports:

1. Choose the **Unit** from the pull-down menu.
2. Choose the port or sequential range of ports using the **From…To…** port pull-down menus.
3. Use the remaining pull-down menus to configure the parameters described below:

Parameter	Description
State <*Enabled*>	Toggle the **State <***Enabled***>** field to either enable or disable a given port.
Speed/Duplex <*Auto*>	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 *Gauto,10/Halfl, 10/Full, 100/Full*, *100/Half, 1000/Full_M,* and *1000Full_Sf.* There is no automatic adjustment of port settings with any option other than *Auto*.

Flow Control	Displays 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 **Disabled**.
Learning	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*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section titled **Forwarding and Filtering** for information on entering MAC addresses into the forwarding table.

Port Mirroring

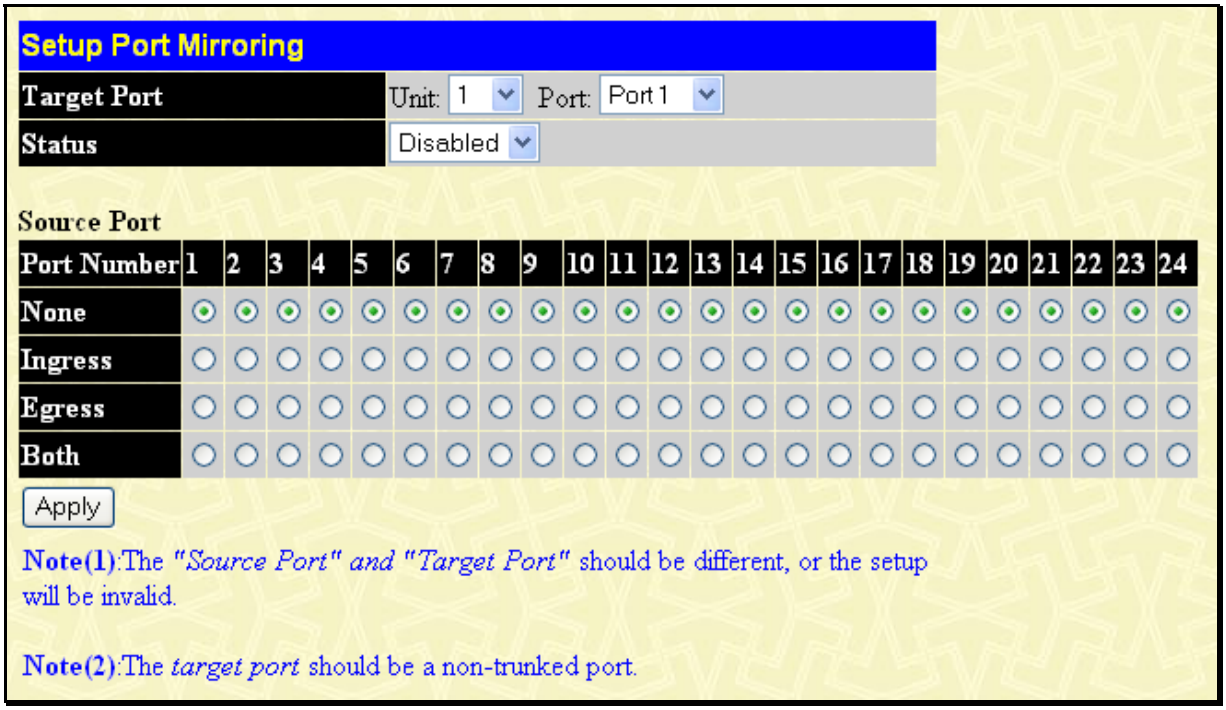


Figure 6-2. Port Mirroring window

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.

To configure a mirror port,

1. Select the **Source Port** from where you want to copy frames and the **Target Port**, which receives the copies from the source port.
2. Select the Source Direction, **Ingress, Egress**, or **Both** and change the **Status** drop-down menu to **Enabled.**
3. Click **Apply** to let the changes take effect.

NOTE: You cannot mirror a fast port onto 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. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

Section 7

Link Aggregation Configuration

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 32 link aggregation groups, each group consisting of up of up to 8 links (ports). A link aggregation group may not cross a 12-port boundary, starting with port 1 (a group may not contain ports 12 and 13, 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.

Port security and 802.1x should not be enabled on any of the aggregated ports. The static multicast group member must be identical among aggregated ports, and the STP port state must be identical among aggregated ports.

The configuration of the Master port in the group becomes the configuration for all of the ports in the 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 the **Link Aggregation** hyperlink in the **Configuration** folder to bring up the **Port Trunk Group Entries** table:

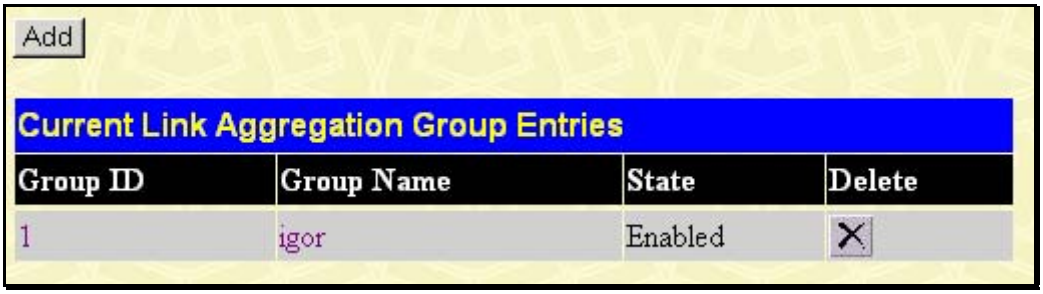


Figure 7-1. Port Trunking Group Entry Table

To configure port trunk groups, click the **Add** button to add a new trunk group and use the menu **Port Trunking Configuration** menu (see example below) to set up trunk groups. To modify a port trunk group, double-click on it to bring up the **Port Trunking Configuration** menu. To delete a port trunk group, click the **Delete** option in the **Port Trunk Group Entries** table.

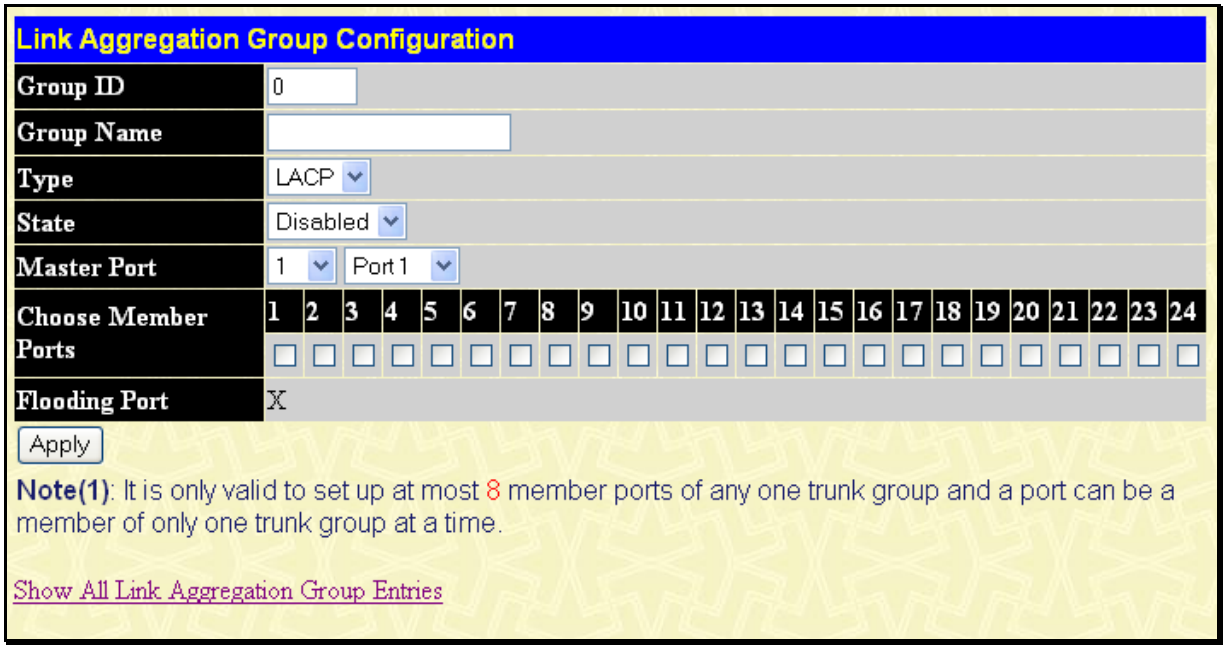


Figure 7-2. Link Aggregation Group Configuration

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group.
Group Name	Type in a name for the group (optional).
State	Trunk groups can be toggled between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Type	This pull-down menu allows you to select between Static and LACP (Link Aggregation Control Protocol.) LACP allows for the automatic detection of links in a Port Trunking Group.
Master Port	Choose the Master port for the trunk group.
Member Unit	Choose the switch unit on which to set up a trunk group. Trunk groups must be confined to ports on a single switch.
Flooding Port	A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts.

Section 8

Forwarding and Filtering

Static Unicast Forwarding

Open the **Forwarding & Filtering** folder in the **Configuration** menu and click on the **Unicast Forwarding** link. This will open the **Setup Static Unicast Forwarding Table**, as shown below.

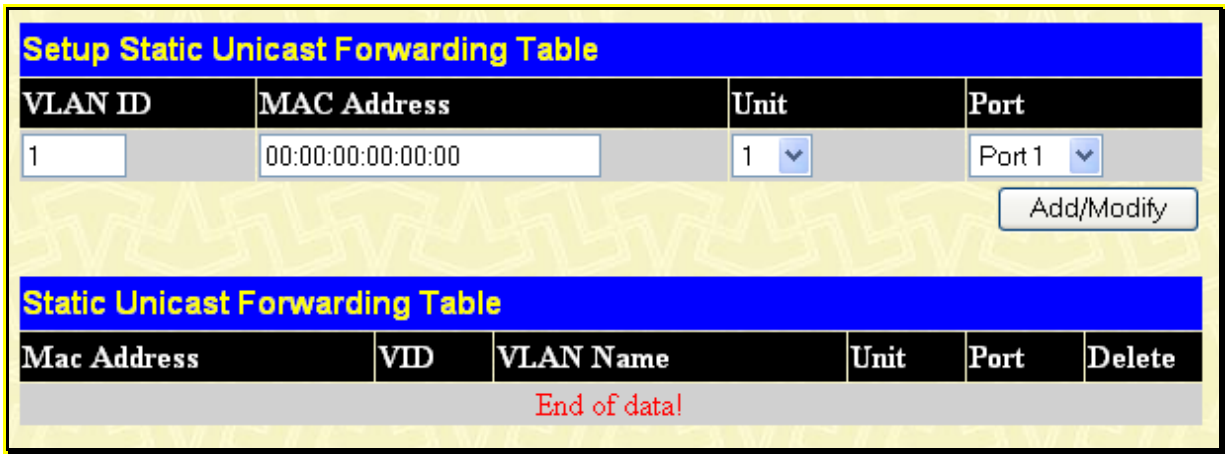


Figure 8-1. Static Unicast Forwarding Setup

To add an entry, define the following parameters in the **Add an Entry** field:

Parameter	Description
VLAN ID	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Allowed to Go to Unit	Allows the designation of the module on which the above MAC address resides.
Port	Choose the port on which the MAC address resides. Selecting Port 0 means no ports are allowed.

Click on the **Add/Modify** button to add a unicast MAC address to the switch's forwarding table, or to modify a previous entry.

Static Multicast Forwarding

The following figure and table describe how to set up Multicast forwarding on the switch. Open the **Forwarding & Filtering** folder and click on the **Multicast Forwarding** link to see the entry screen below:

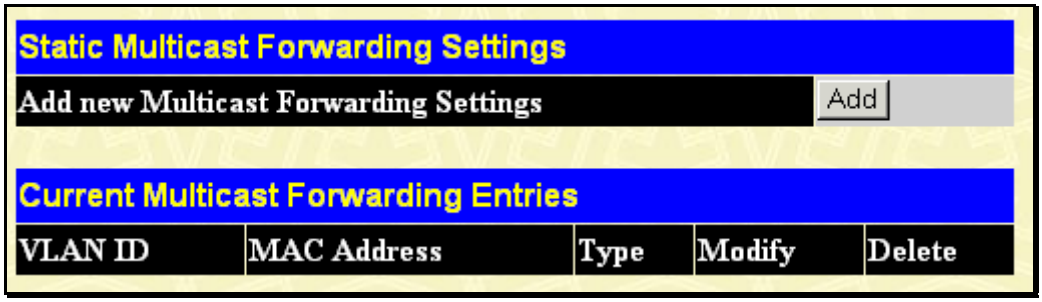


Figure 8-2. Setup Static Multicast Forwarding Table

The Static Multicast Forwarding Settings page displays all of the entries made into the switch's static multicast forwarding table. Click the **Add** button to open the **Setup Static Multicast Forwarding Table**, as shown below.

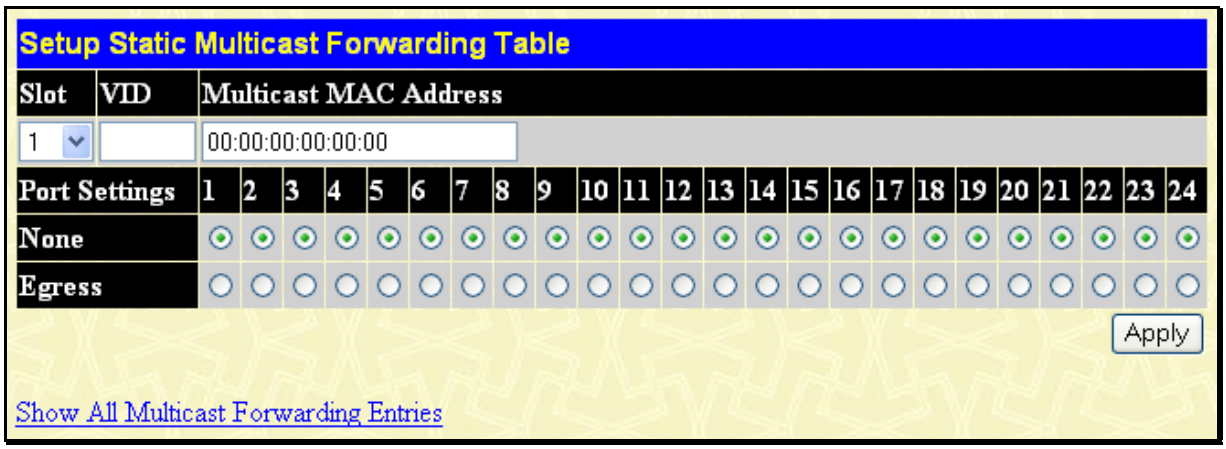


Figure 8-3. Setup Static Multicast Forwarding Table

The following parameters can be set:

Parameter	Description
MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
VID	The VLAN ID of the VLAN the above MAC address belongs to.
Port Settings	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are; None – no restrictions on the port dynamically joining the multicast group, None is chosen, then an end station attached to the port can join the multicast group using GMRP. **Egress** – the port is a static member of the multicast group.

Section 9

IGMP Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch (see **Advanced Settings**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping** link in the **Configuration** folder. When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

Use the IGMP Snooping Group Entry Table to view IGMP Snooping status. To modify settings, click the Modify button for the VLAN ID you want to change.

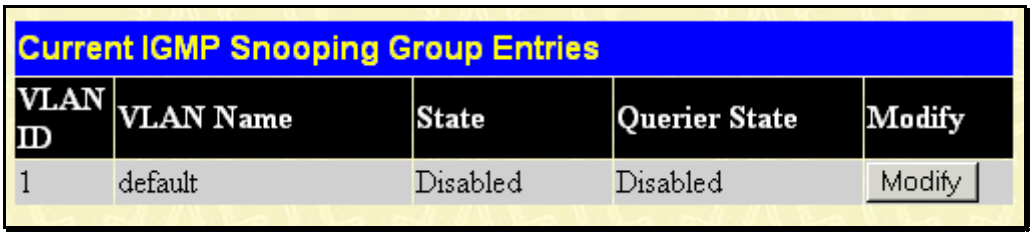


Figure 9-4. IGMP Snooping Entry Table

Clicking the **Modify** button will bring up the IGMP Snooping Settings menu.

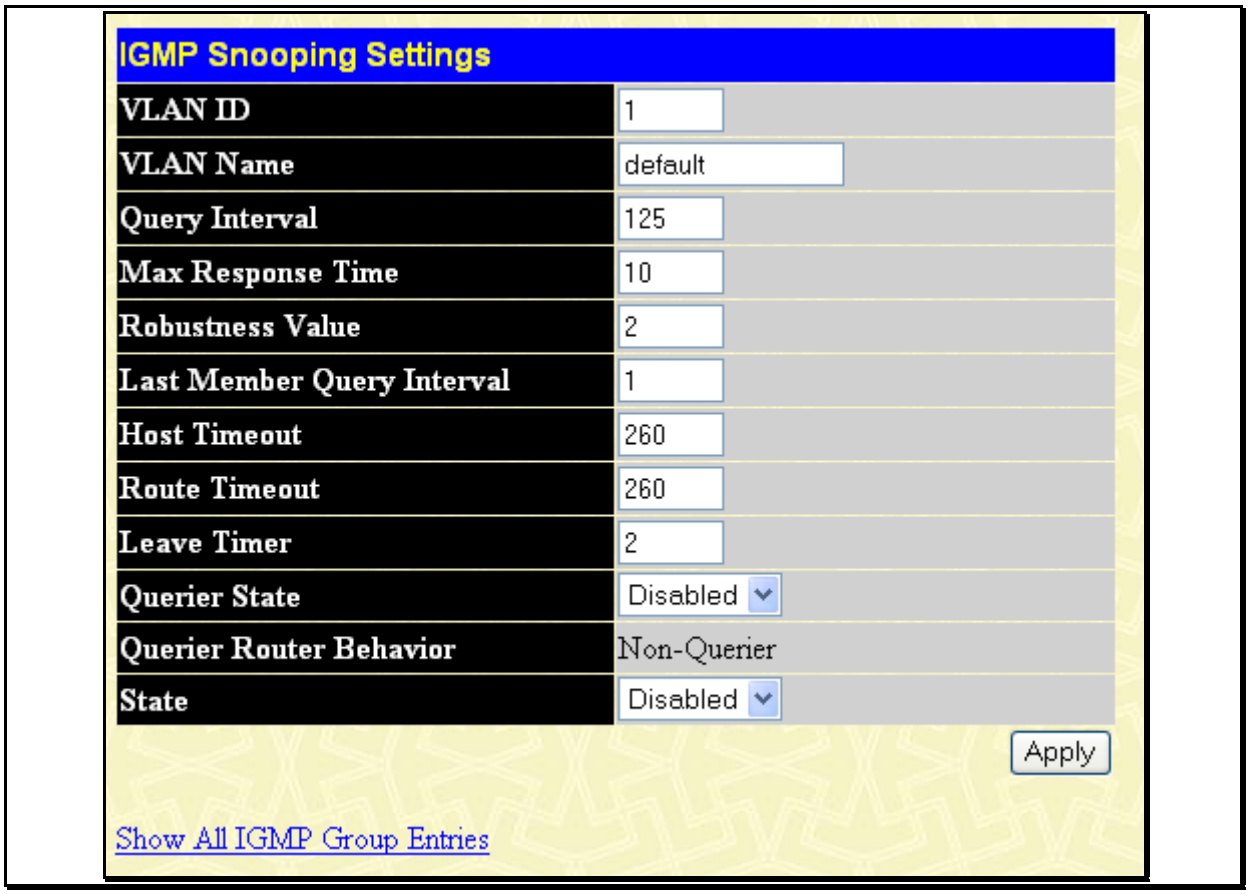


Figure 9-5. IGMP Snooping Settings Screen

Parameter	Description
Query Interval	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 9,999 seconds are allowed. Default = 125.
Max Response Time	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = 10.
Robustness Variable	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of 2 to 255. Default = 2.
Last Member Query Interval	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = 1.
Host Timeout	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = 260.
Route Timeout	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = 260.
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.
Querier State	Choose *Querier* to enable transmitting IGMP Query packets or *Non-Querier* to disable. The default value is *Non-Querier*.
State	Select *Enabled* to implement IGMP Snooping. This is *Disabled* by default.

Static Router Ports

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages (IGMP) coming from the network to be propagated to the router.

A router port has the following behavior:

- All IGMP Report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of the Layer 3 switch would not be able to receive UDP data streams unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast, PIM-DM multicast packets are detected flowing into a port.

Open the **IGMP** folder and the click on the Static Router Ports Entry link to open the **Current Static Router Ports Entries** page, as shown below.

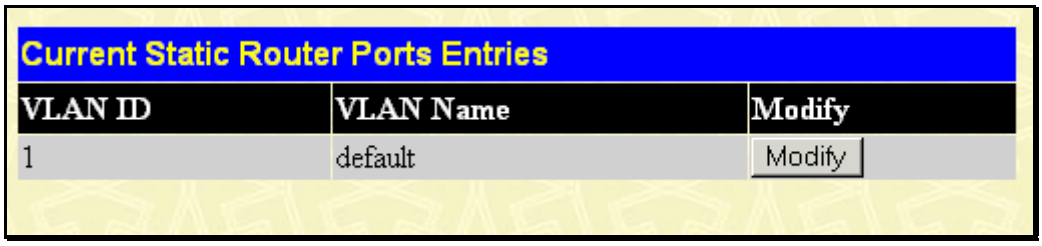


Figure 9-6. Current Static Router Ports Screen

The Current Static Router Ports Entries page (shown above) displays all of the current entries to the Switch's static router port table. To add or modify an entry, click the **Modify** button. This will open the **Static Router Ports Settings** page, as shown below.

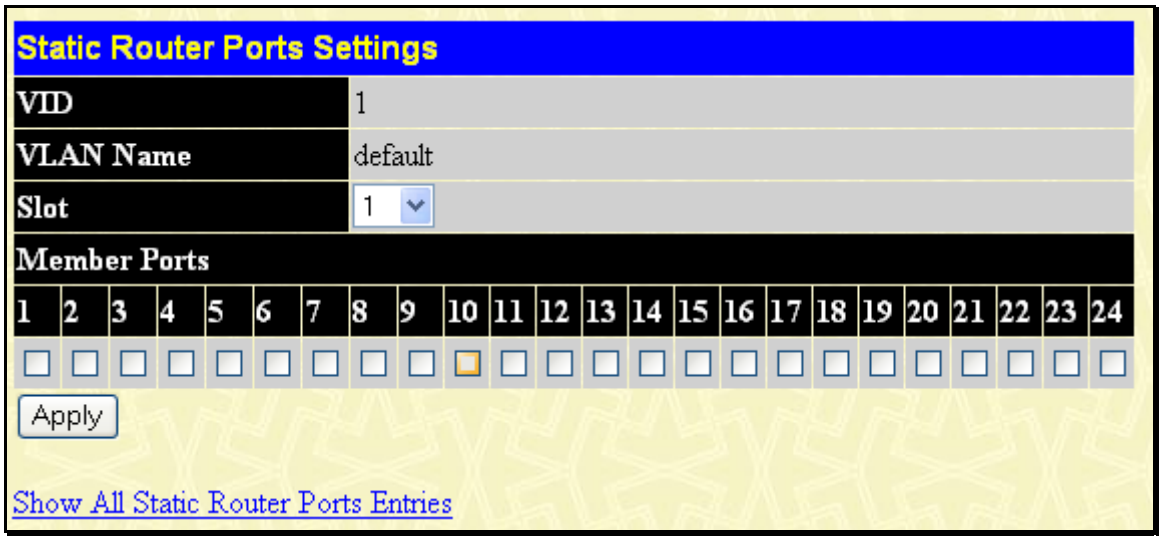


Figure 9-7. Static Router Ports Settings Screen

The following parameters can be set:

Parameter	Description
VID (VLAN ID)	This is the VLAN ID that, along with the VLAN name, identifies the VLAN where the multicast router is attached.
VLAN Name	This is the name of the VLAN where the multicast router is attached.
Unit	This is the Unit ID of the switch in a switch stack for which you are creating an entry into the switch's static router port table.
Member Ports	There are the ports on the switch that will have a multicast router attached to them.

New IGMP Snooping Feature

In the DGS-3224SR, the user may configure a forbidden portlist, whose members are not forced to become router ports.

To activate this feature, please use the console (CLI). The CLI command will be:

Config router_ports_forbidden

To disp[lay the forbidden portlist, the CLI command will be:

Show router_ports

Section 10

Spanning Tree Protocol Configuration

The switch supports 802.1d Spanning Tree Protocol (STP) and 802.1w Rapid Spanning Tree Protocol (RSTP). 802.1d STP will be familiar to most networking professionals. However since 802.1w RSTP has been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1 d STP and 802.1w RSTP.

802.1w Rapid Spanning Tree

The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEE 802.1w specification and a version compatible with the IEEE 802.1d STP. RSTP can operate with legacy equipment implementing IEEE 802.1d, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 function that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the two protocols is in the way ports transition to a forwarding state and the in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. RSTP combines the transition states disabled, blocking and listening used in 802.1d and creates a single state *Discarding*. In either case, ports do not forward packets; in the STP port transition states disabled, blocking or listening or in the RSTP port state discarding there is no functional difference, the port is not active in the network topology. Table 5-7 below compares how the two protocols differ regarding the port state transition.

Both protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently – with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges are sensitive to the status of the link. Ultimately this difference results faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1d is this absence of immediate feedback from adjacent bridges.

802.1d STP	802.1w RSTP	Forwarding?	Learning?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

Comparing Port States

RSTP is capable of more rapid transition to a forwarding state – it no longer relies on timer configurations – RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and

learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1d/802.1w Compatibility

RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1d format when necessary. However, any segment using 802.1 STP will not benefit from the rapid transition and rapid topology change detection of RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP.

STP Switch Settings

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 of ports basis.

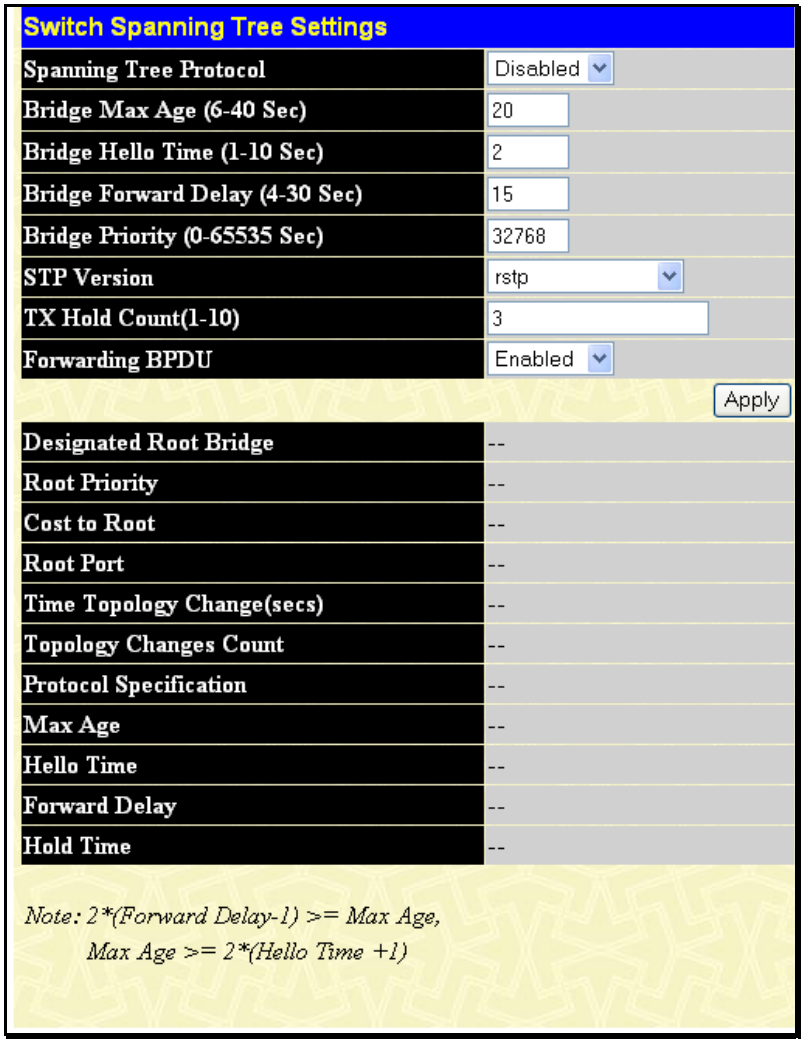


Figure 10-1. STP Switch Settings

Configure the following parameters and click the Apply button to implement them:

Parameter	Description
Status <*Disabled*>	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. This will enable or disable the Spanning Tree Protocol (STP), globally, for the switch.
Max Age: (6 - 40 sec) <*20* >	The Max. Age can be set from 6 to 40 seconds. At the end of the Max. 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 set 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.
Forward Delay: (4 - 30 sec) <*15* >	The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.
Priority: (0 - 61440) <*32768*>	A Priority for the switch can be set from 0 to 61440. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch.
STP Version<*RSTP* >	Choose RSTP (default) or STP Compatibility. Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment.
Tx Hold Count <*3* >	This is the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. Default value = 3.
Forwarding BPDU <*Enabled* >	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: the Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

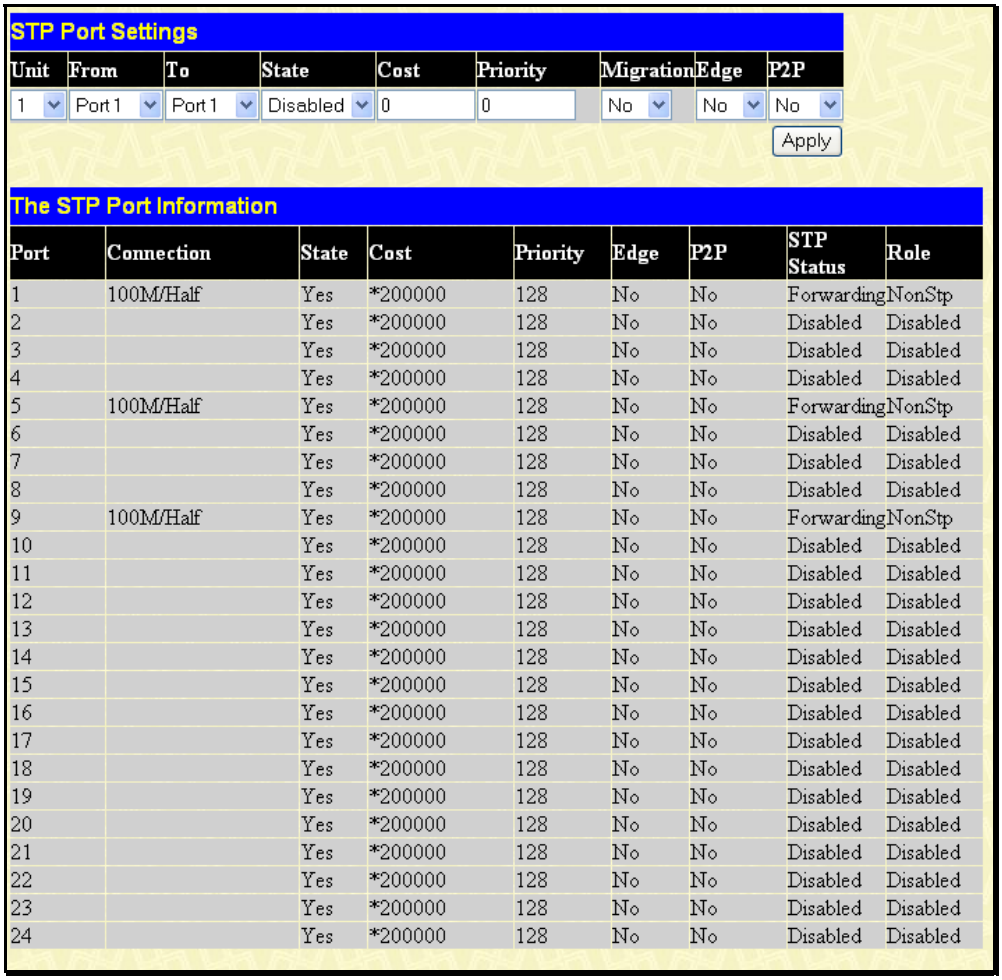
Observe the following formulas when setting the above parameters:

Max. Age ≤ 2 x (Forward Delay - 1 second)

Max. Age ≥ 2 x (Hello Time + 1 second)

STP Port Settings

For stacked switch installations, first select the Unit to be configured.



STP Port Settings

Unit	From	To	State	Cost	Priority	Migration	Edge	P2P
1	Port 1	Port 1	Disabled	0	0	No	No	No

Apply

The STP Port Information

Port	Connection	State	Cost	Priority	Edge	P2P	STP Status	Role
1	100M/Half	Yes	*200000	128	No	No	Forwarding	NonStp
2		Yes	*200000	128	No	No	Disabled	Disabled
3		Yes	*200000	128	No	No	Disabled	Disabled
4		Yes	*200000	128	No	No	Disabled	Disabled
5	100M/Half	Yes	*200000	128	No	No	Forwarding	NonStp
6		Yes	*200000	128	No	No	Disabled	Disabled
7		Yes	*200000	128	No	No	Disabled	Disabled
8		Yes	*200000	128	No	No	Disabled	Disabled
9	100M/Half	Yes	*200000	128	No	No	Forwarding	NonStp
10		Yes	*200000	128	No	No	Disabled	Disabled
11		Yes	*200000	128	No	No	Disabled	Disabled
12		Yes	*200000	128	No	No	Disabled	Disabled
13		Yes	*200000	128	No	No	Disabled	Disabled
14		Yes	*200000	128	No	No	Disabled	Disabled
15		Yes	*200000	128	No	No	Disabled	Disabled
16		Yes	*200000	128	No	No	Disabled	Disabled
17		Yes	*200000	128	No	No	Disabled	Disabled
18		Yes	*200000	128	No	No	Disabled	Disabled
19		Yes	*200000	128	No	No	Disabled	Disabled
20		Yes	*200000	128	No	No	Disabled	Disabled
21		Yes	*200000	128	No	No	Disabled	Disabled
22		Yes	*200000	128	No	No	Disabled	Disabled
23		Yes	*200000	128	No	No	Disabled	Disabled
24		Yes	*200000	128	No	No	Disabled	Disabled

Figure 10-2. STP Port Settings

In addition to setting Spanning Tree parameters for use on the switch level, the switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected on the basis of port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The following fields can be set:

Parameter	Description
Unit	This is the Unit ID of a switch in a switch stack. 15 indicates a DGS-3224SR switch in standalone mode.
From/To	A consecutive group of ports may be configured starting with the selected port.
State	This drop-down menu allows you to **Enable** or **Disable** STP for the selected group of ports.
Cost	A Port Cost can be set from *1* to *200000000*. The lower the number, the greater the probability the port will be chosen to forward packets. Default port cost: 100Mbps port = 200000 Gigabit ports = 20000
Priority <*128*>	A Port Priority can be from *0* to *240*. The lower the number, the greater the probability the port will be chosen as the Root Port.
Migration <*No*>	Select Yes or No. Choosing Yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.
Edge <*No*>	Select Yes or No. Choosing Yes designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. No indicates the port does not have edge port status.
P2P <*Yes*>	Select Yes or No. Choosing Yes indicates a point-to-point (p2p) shared link. These are similar to edge ports however they are restricted in that a p2p port must operate in full-duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP.

Section 11

QoS (Quality of Service)

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. In 802.1p compliant devices, a tag inserted into the packet header is used to identify the priority level of data packets.

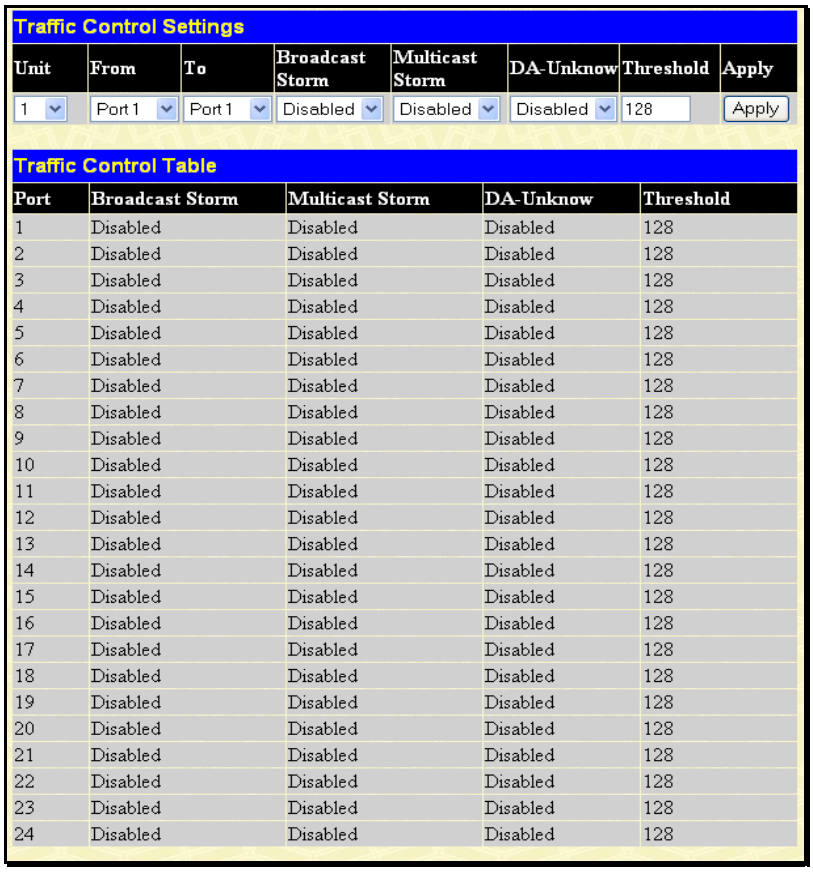
The Switch implements 802.1p priority using 8 hardware queues. *Note:*

Individual ports may still be assigned priority using the 8 levels as defined by the 802.1p standard.

It is important to note that changes in a networks QoS scheme should be carefully considered, planned for and if possible tested for efficiency. When set up properly, it QoS can allow efficient and timely delivery of data for video conferencing or IP telephony without causing unacceptable delays of other network traffic. If QoS is not well set up however, significant delays and excessive packet loss may result for data assigned to lower priority queues.

Traffic Control (Broadcast/Multicast Storm Control)

Use the Traffic Control Setting menu to enable or disable storm control and adjust the threshold for multicast and broadcast storms, as well as DLF (Destination Look Up Failure). Traffic control settings are applied to individual Switch modules.



Traffic Control Settings

Unit	From	To	Broadcast Storm	Multicast Storm	DA-Unknow	Threshold	Apply
1	Port 1	Port 1	Disabled	Disabled	Disabled	128	Apply

Traffic Control Table

Port	Broadcast Storm	Multicast Storm	DA-Unknow	Threshold
1	Disabled	Disabled	Disabled	128
2	Disabled	Disabled	Disabled	128
3	Disabled	Disabled	Disabled	128
4	Disabled	Disabled	Disabled	128
5	Disabled	Disabled	Disabled	128
6	Disabled	Disabled	Disabled	128
7	Disabled	Disabled	Disabled	128
8	Disabled	Disabled	Disabled	128
9	Disabled	Disabled	Disabled	128
10	Disabled	Disabled	Disabled	128
11	Disabled	Disabled	Disabled	128
12	Disabled	Disabled	Disabled	128
13	Disabled	Disabled	Disabled	128
14	Disabled	Disabled	Disabled	128
15	Disabled	Disabled	Disabled	128
16	Disabled	Disabled	Disabled	128
17	Disabled	Disabled	Disabled	128
18	Disabled	Disabled	Disabled	128
19	Disabled	Disabled	Disabled	128
20	Disabled	Disabled	Disabled	128
21	Disabled	Disabled	Disabled	128
22	Disabled	Disabled	Disabled	128
23	Disabled	Disabled	Disabled	128
24	Disabled	Disabled	Disabled	128

Figure 10-3. Traffic Control Settings

Traffic or storm control is used to stop broadcast, multicast or ARP request storms that may result when a loop is created. The Destination Look Up Failure control is a method of shutting down a loop when a storm is formed

because a MAC address cannot be located in the Switch's forwarding database and it must send a packet to all ports or all ports on a VLAN.

To configure Traffic Control, select the **Unit** (Unit ID of a switch in a switch) you want to configure. **Broadcast Storm**, **Multicast Storm** and **Destination Look Up Failure** may be *Enabled* or *Disabled*. The **Threshold** value is the upper threshold at which the specified traffic control is switched on. This is the number of Broadcast, Multicast or DLF packets, in Kbps, received by the switch that will trigger the storm traffic control measures. The Threshold value can be set from 0 to 255 packets. The Default setting is 128.

Configuring Default Priority

The switch allows the assignment of a default 802.1p priority to each port on the switch.

Click on the **802.1p Default Priority** link:

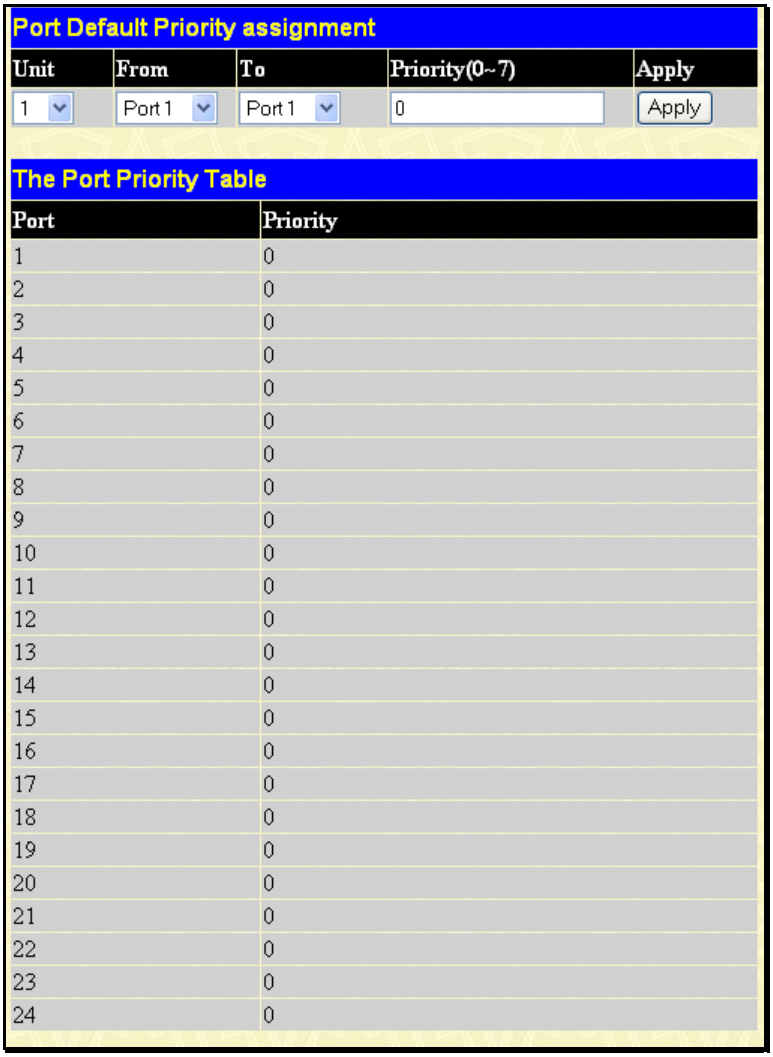


Figure 10-4. Priority Based on a Port-group basis

This page allows you to assign a default 802.1p priority to any given port on the switch. The priority queues are numbered from 0 – the lowest priority – to 7 – the highest priority.

Configuring 802.1p User Priority

The DGS-3224SR allows the assignment of a User Priority to each of the 802.1p priorities.

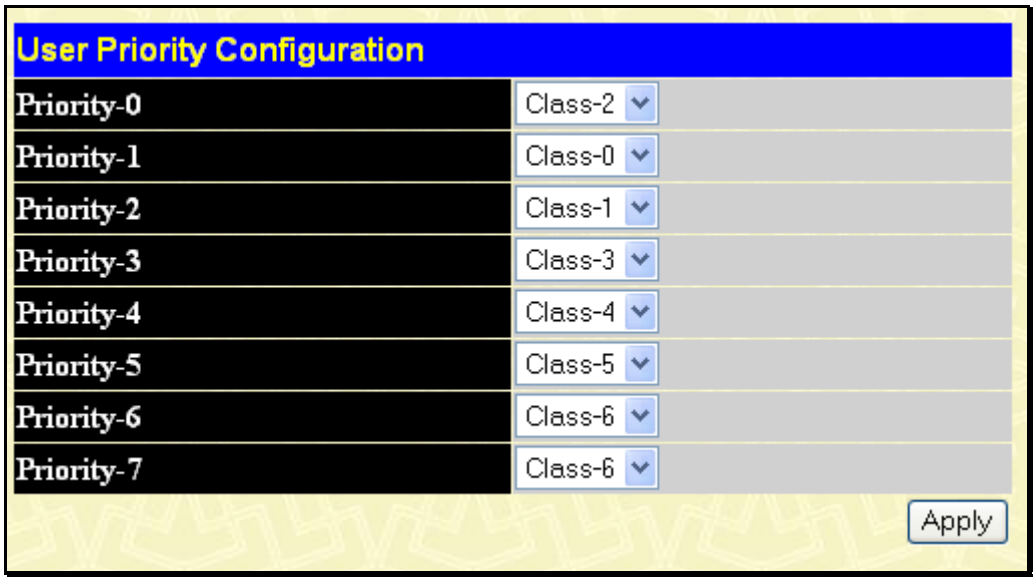


Figure 10-5. User Priority Configuration

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.

QoS Output Scheduling Configuration

QoS can be customized by changing the output scheduling used for the hardware queues in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand as bottlenecks can quickly develop if the QoS settings are not suitable.

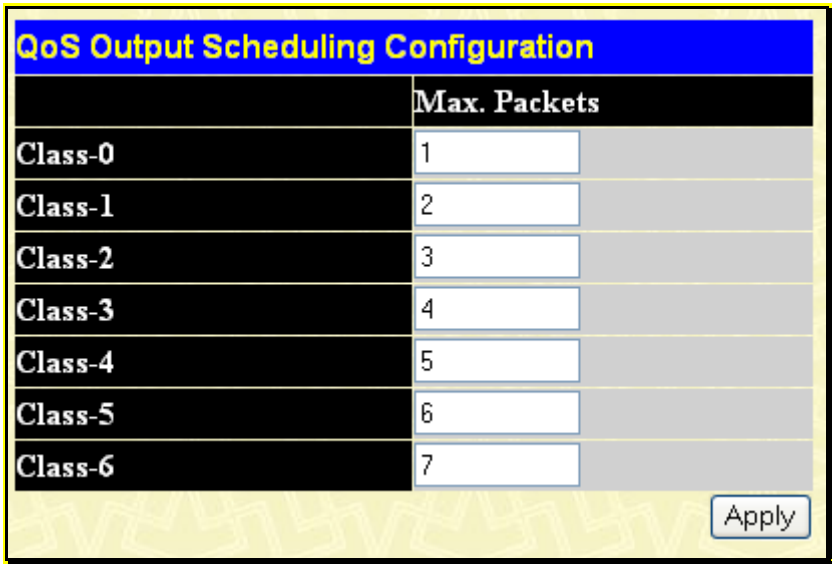
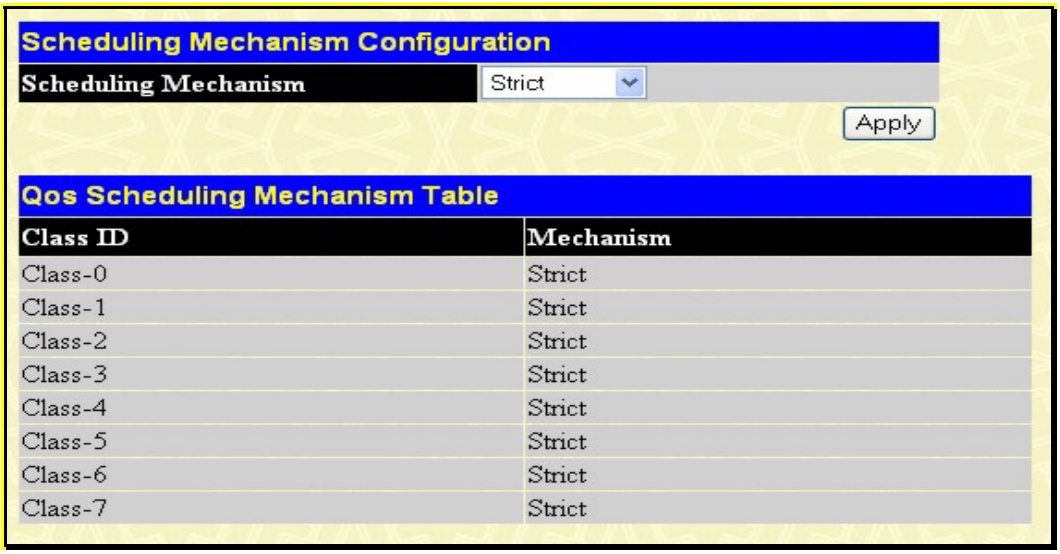


Figure 10-6. QoS Output Scheduling Configuring

Scheduling Mechanism – This drop-down menu allows you to select between a **Weight Fair** and a **Strict** mechanism for emptying the priority queues.



Click **Apply** to let your changes take effect.

802.1p User Priority

The User Priority menu is used to map incoming packets with 802.1p priority tags to one of the 8 hardware queues used on the Switch.

Note: Level 7 (the highest level) is reserved for internal control packets.

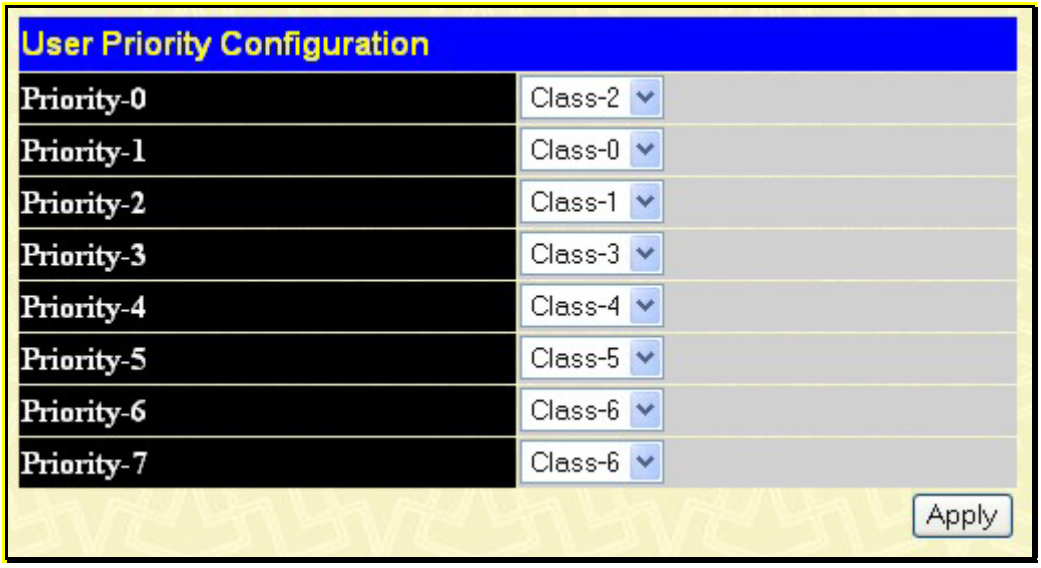


Figure 10-7. Traffic Class Configuration window

This window allows you to configure traffic class priority by specifying the class value, from 0 to 6, of the Switch's eight levels of priority.

Click **Apply** to let your changes take effect.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on either a single switch (in standalone mode) or a group of ports on another switch in a switch stack. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Master switch CPU.

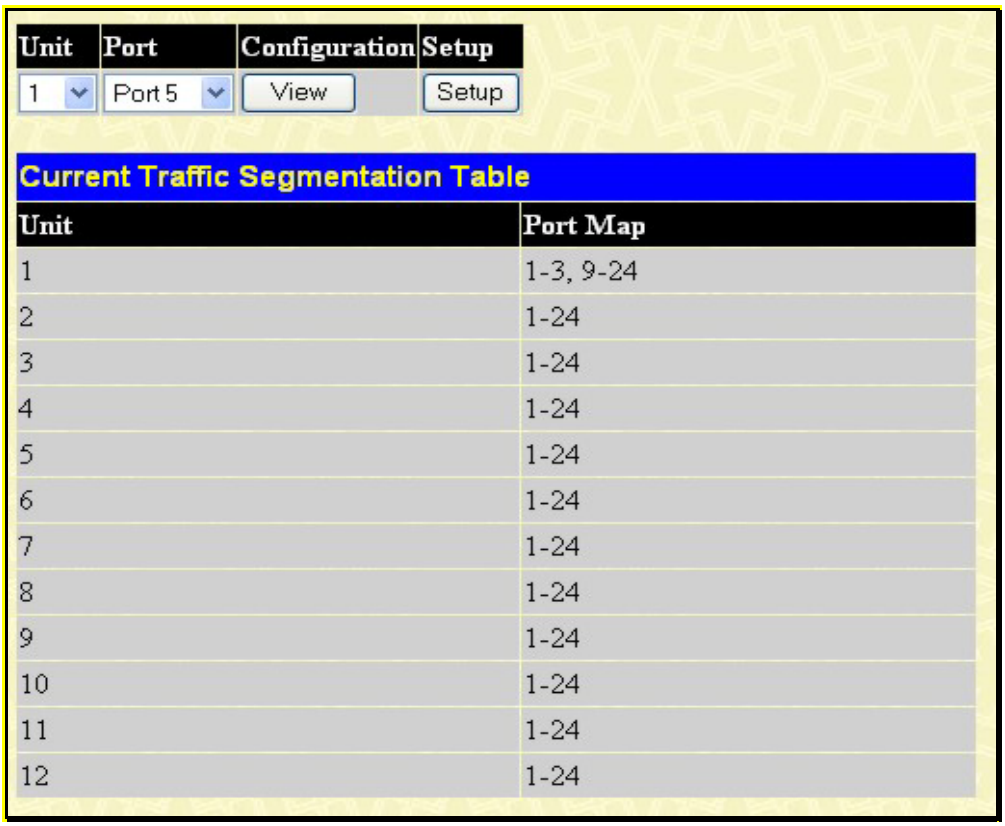


Figure 10-8. Traffic Segmentation Table

Click on the **Setup** button to open the **Setup Forwarding ports** page, as shown below.

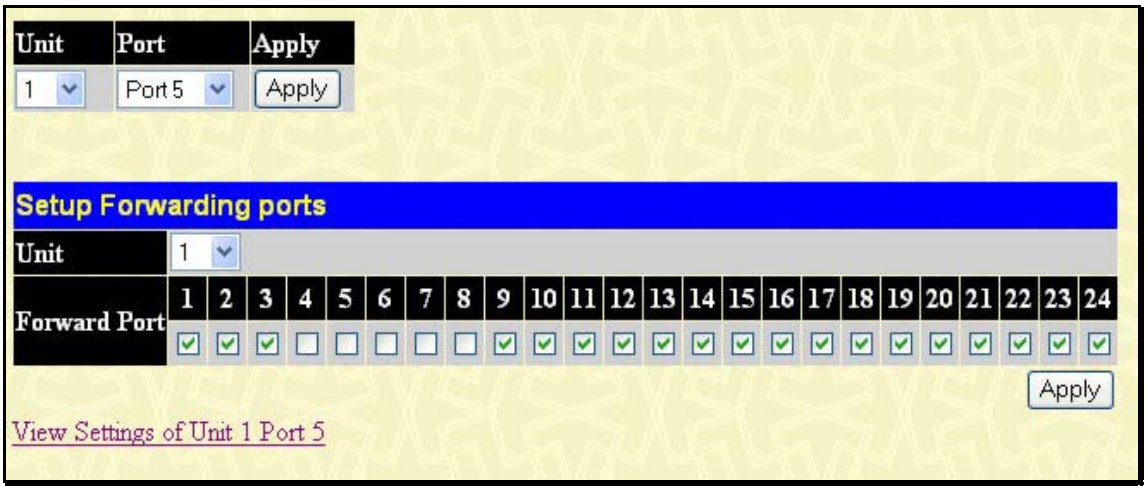


Figure 10-9. Setup Forwarding Ports

This page allows you to determine which port on a given switch in a switch stack will be allowed to forward packets to other ports on that switch.

Configuring traffic segmentation on the DGS-3224SR is accomplished in two parts. First you specify a switch from a switch stack, and then a port from that switch. Then you specify a second switch from the switch stack, and then you select which ports (or different ports on the same switch,) on that switch that you want to be able to receive packets from the switch and port you specified in the first part.

In the example above, the switch is Unit 1 and port 5 is selected as the transmitting port. Ports 1-3 and 9-24 are selected as being able to receive packets from port 5.

Clicking the **Apply** button will enter the combination of transmitting port and allowed receiving ports into the switch's Traffic Segmentation table.

The **Unit** drop-down menu at the top of the page allows you to select a switch from a switch stack using that switch's Unit ID. The **Port** drop-down menu allows you to select a port from that switch. This is the port that will be transmitting packets.

The **Unit** drop-down menu under the Setup Forwarding ports heading allows you to select a switch from a switch stack using that switch's Unit ID. The **Forward Port** click boxes allow you to select which of the ports on the selected switch will be able to forward packets. These are the ports that will be allowed to receive packets from the port specified above.

Click **Apply** to enter the settings into the switch's Traffic Segmentation table.

Bandwidth Control

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

Bandwidth Settings

Unit	From	To	Type	no_limit	Rate	Apply
1	Port 1	Port 1	Both	Disabled	1	Apply

Port Bandwidth Table

Port	RX Rate (Mbit/sec)	TX Rate (Mbit/sec)
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 10-11. Bandwidth Settings

The following parameters can be set or are displayed:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID.
From/To	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select between **RX** (receive,) **TX** (transmit,) and **Both**. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
no_limit	This drop-down menu allows you to specify that the selected port will have no bandwidth limit. **Enabled** disables the limit.
Rate	This field allows you to enter the data rate, in kb/s, that will be the limit for the selected port.

Section 12

System Log Server

The switch can send Syslog messages to up to four designated servers. Use the System Log Server

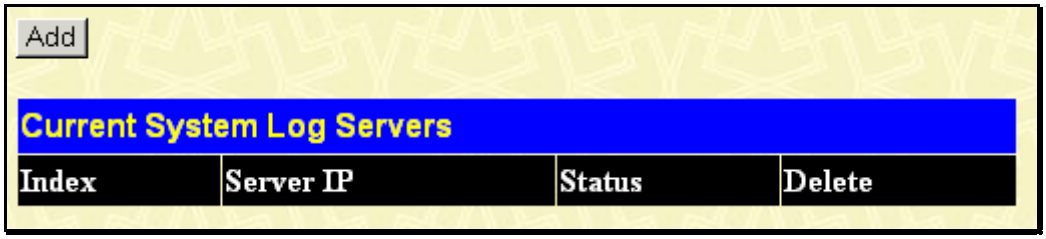


Figure 13-1. System Log Servers

The parameters configured for adding and editing System Log Server settings are the same. See the table below for a description.

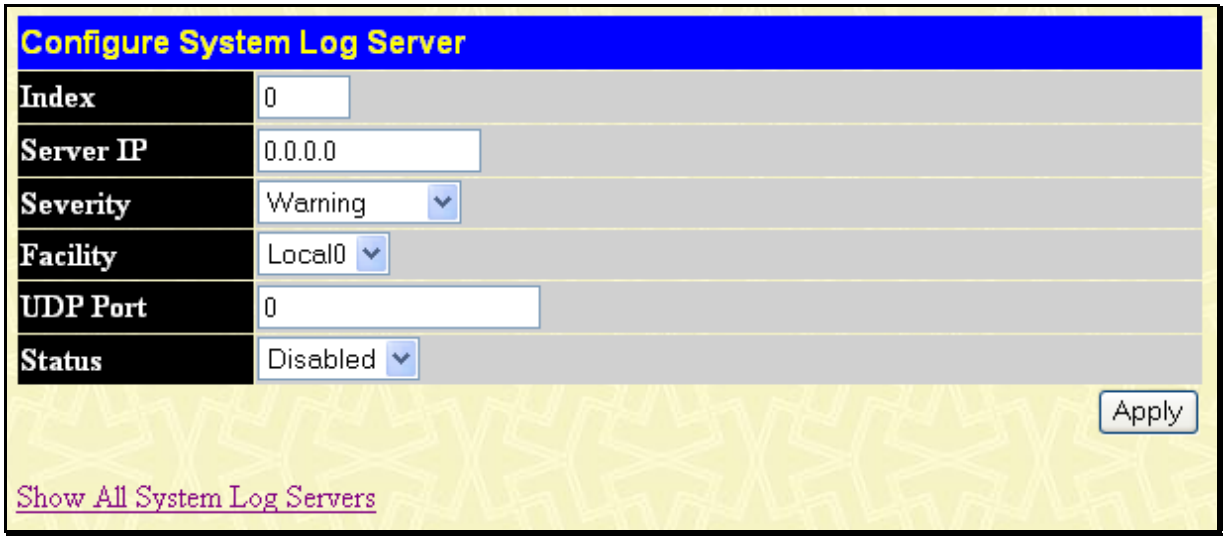


Figure 13-2. System Log Servers – Add

The following parameters can be set:

Parameter	Description
Index	Syslog server settings index (1-4).
Server IP	The IP address of the Syslog server.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are **Warning, Informational**, and **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 that the switch currently now. Numerical Facility Code 0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog line printer subsystem 7 network news subsystem 8 UUCP subsystem 9 clock daemon 10 security/authorization messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon **16 local use 0 (local0)** **17 local use 1 (local1)** **18 local use 2 (local2)** **19 local use 3 (local3)** **20 local use 4 (local4)** **21 local use 5 (local5)** **22 local use 6 (local6)** **23 local use 7 (local7)**
UDP Port	Type the UDP port number used for sending Syslog messages. The default is 514.
Status	Choose Enabled or Disabled to activate or deactivate this

Section 13

Port Security Settings

A given port's (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. The port can be locked by using the **Learn** <*Disabled*> pull-down menu to *Enabled*, and clicking **Apply**.

This is a security feature that prevents unauthorized computers (with source MAC addresses unknown to the switch prior to locking the port (or ports) from connecting to the switch's locked ports and gaining access to the network.

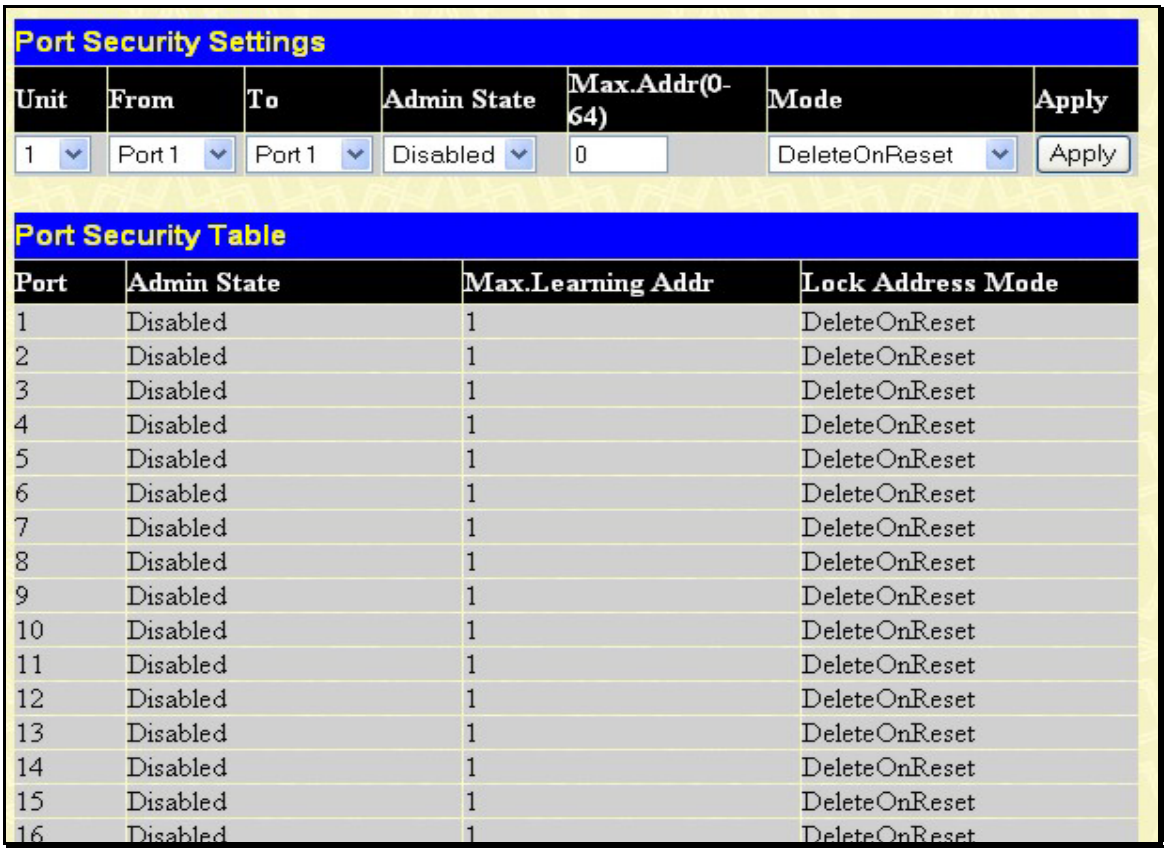


Figure 14-1. Port Security Settings

The following parameters can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID.
From/To	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows you to **Enable** or **Disable** Port Security (locked MAC address table for the selected ports.)
Max.Addr(0-64)	The number of MAC addresses that will be in the MAC address forwarding table for the selected switch and group of ports.

Mode	This pull-down menu allows you to select how the MAC address table locking will be implemented on the switch, for the selected group of ports. The options are **DeleteOnReset** and **DeleteOnTimeout**.

Section 14

SNTP Setting

The Simple Network Time Protocol (SNTP) (an adaptation of the Network Time Protocol (NPT) is configured on the switch using the following pages.

Time Settings

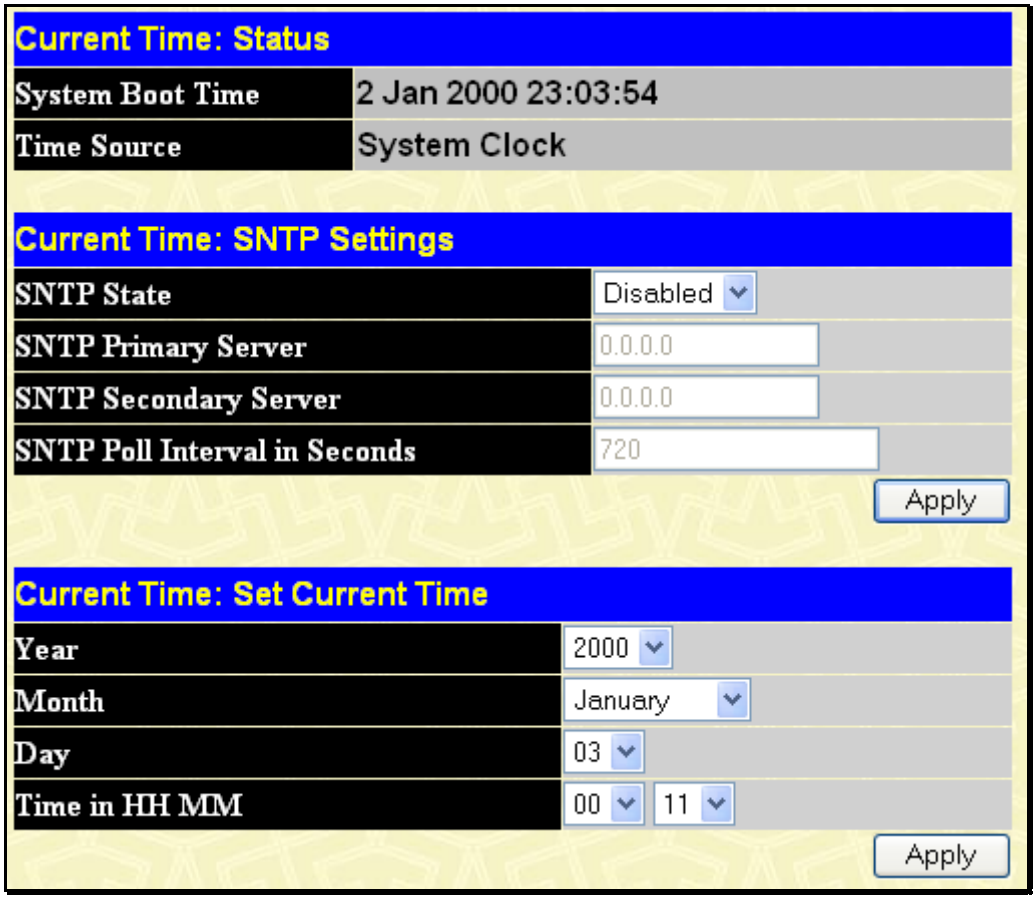


Figure 15-1. Time Settings Page

The following parameters can set or are displayed:

Parameter	Description
System Boot Time	Displays the current system time.
Time Source	Displays the time source for the system.
SNTP State	Use this pull-down menu to **Enable** or **Disable** SNTP.
SNTP Primary Server	This is the primary server the SNTP information will be taken from
SNTP Secondary Server	This is the secondary server the SNTP information will be taken from
SNTP Poll Interval in	This is the interval between requests for updated SNTP information.

Seconds	
Year	Enter the current year, if you want to update the system clock.
Month	Enter the current month, if you want to update the system clock.
Day	Enter the current day, if you want to update the system clock.
Time in HH MM SS	Enter the current time in hours, minutes, and seconds, if you want to update the system clock.

Time Zone and DST

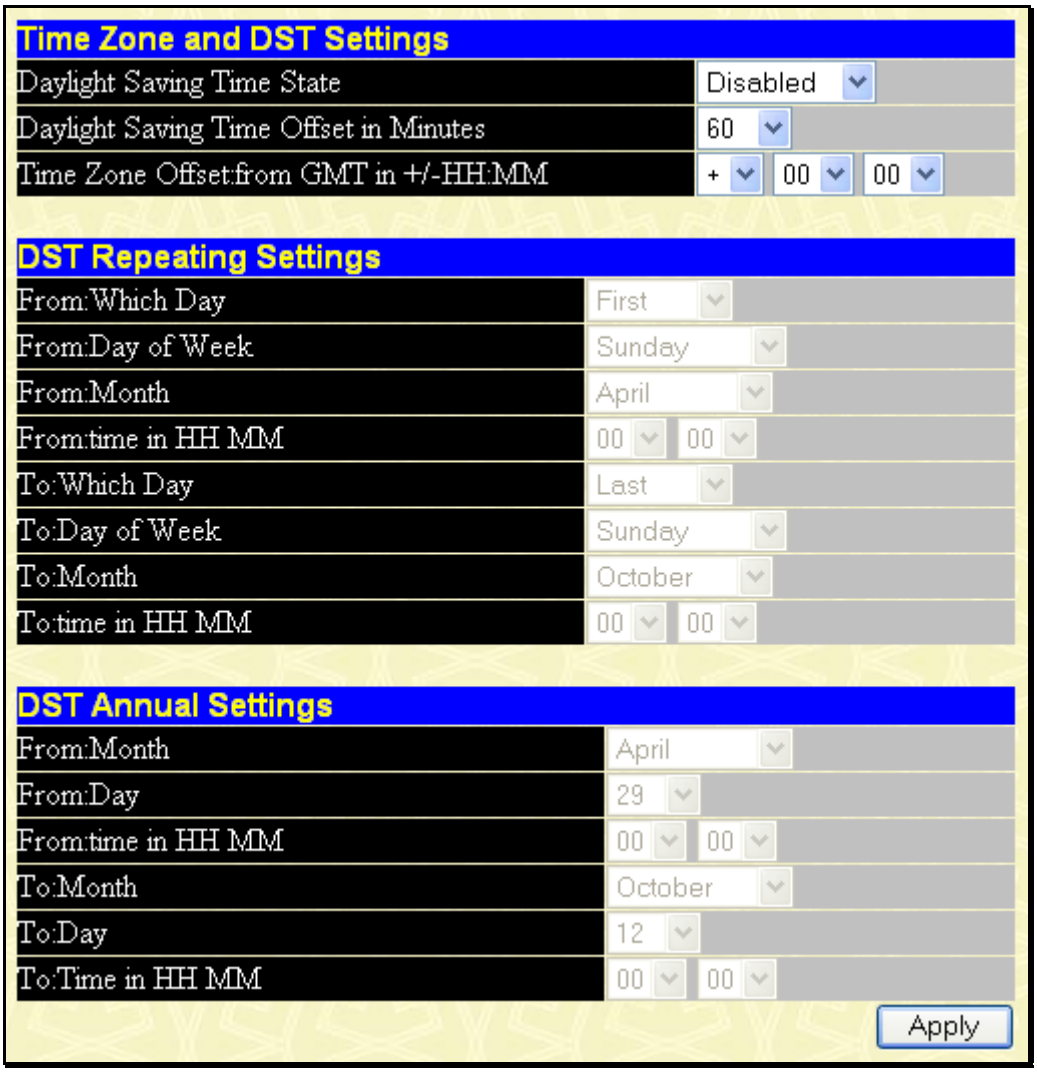


Figure 15-2. Time Zone and DST Settings Page

The following parameters can set:

Parameter	Description
Daylight Saving Time State	Use this pull-down menu to **Enable** or **Disable** the DST Settings.
Daylight Saving	Use this pull-down menu to specify the amount of time that will

Time Offset in Minutes	constitute your local DST offset – 30, 60, 90, or 120 minutes.
Time Zone Offset from GMT in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)
DST Repeating Settings	Repeating - Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.
From: Which Day	Should be From: Which Week. Enter the week of the month that DST will start.
From: Day of Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: time in HH:MM	Enter the time of day that DST will start on.
To: Which Day	Should be be To: Which Week. Enter the week of the month the DST will end.
To: Day of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: time in HH:MM	Enter the time DST will end.
Annual Settings	Annual - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified consisely. For example, specify to begin DST on April 3 and end DST on October 14.
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the week DST will start on, each year.
From: time in HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the day of the week DST will end on, each year.
To: time in HH:MM	Enter the time of day that DST will end on, each year.

Section 15

Access Profile Table

Access profiles allow you to establish criteria to determine whether or not the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address or IP address.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the switch will use to determine what to do with the frame. The entire process is described below in two parts.

To display the currently configured Access Profiles on the switch, open the **Configuration** folder and click on the **Access Profile** Table link. This will open the **Access Profile Table** page, as shown below.

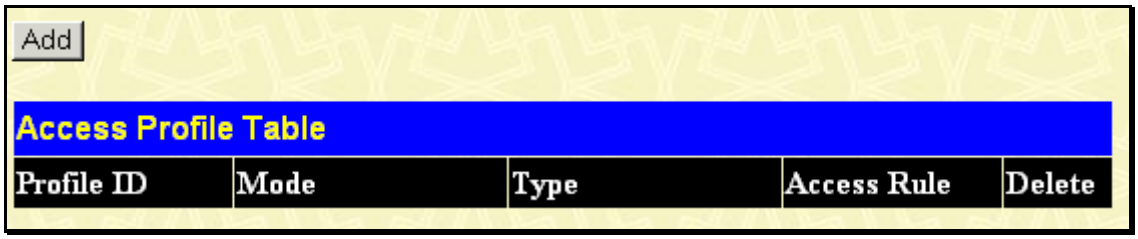


Figure 16-1. Access Profile Table

To add an entry to the **Access Profile Table**, click the **Add** button. This will open the **Access Profile Configuration** page, as shown below. There are two **Access Profile Configuration** pages – one for **Ethernet** (or MAC address-based) profile configuration, and one for **IP** address-based profile configuration. You can switch between the two **Access Profile Configuration** pages by using the **Type** drop-down menu, and clicking on the **Apply** button. The page shown below is the **Ethernet Access Profile Configuration** page.

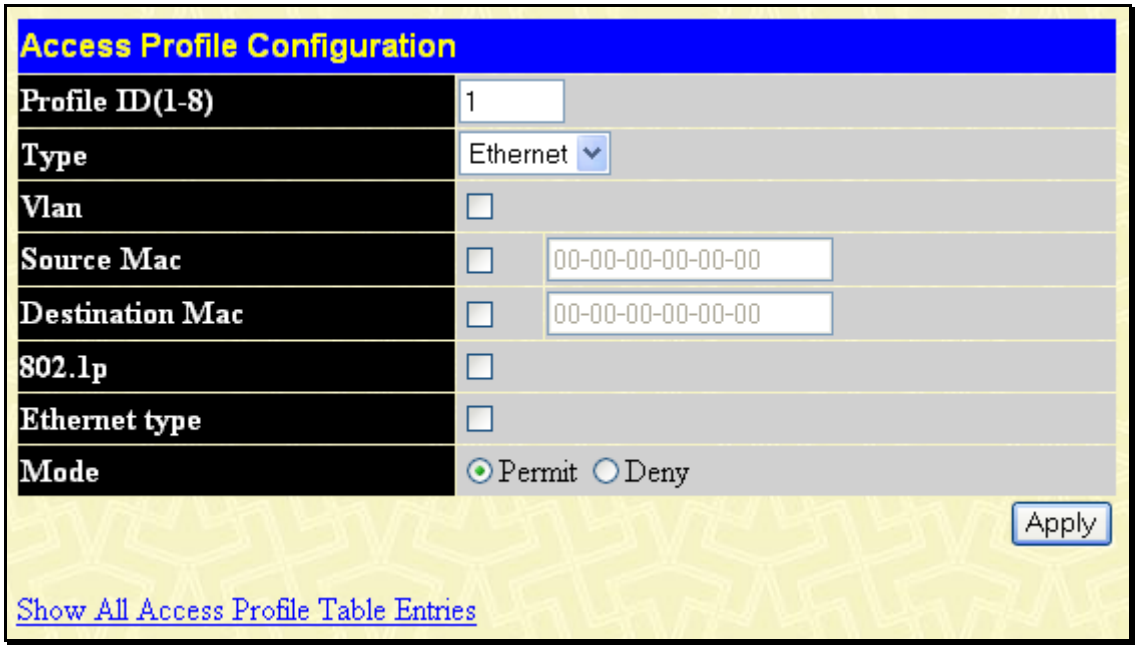


Figure 16-2. Access Profile Table (Ethernet)

The following parameters can be set:

Parameter	Description
Profile ID(1-8)	Type in a unique identifier number for this profile set or allow an ID to be automatically assigned by checking the Auto Assign option. This value can be set from 1 – 8.
Type	Select profile based on Ethernet (MAC Address) or IP address. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the switch to examine the layer 2 part of each packet header. Select IP to instruct the switch to examine the IP address in each frame's header.
Vlan	Selecting this option instructs the switch to examine the VLAN part of each packet header and use this as the full or partial criterion for forwarding.
Source Mac	Source MAC Mask - Enter a MAC address mask for the source MAC address.
Destination Mac	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
802.1p	Selecting this option instructs the switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet type	
Mode	Select permit to specify that the packets that match the access profile are forwarded by the switch according to any additional rule added (see below). Select deny to specify that packets that do not match the access profile are not forwarded by the switch and will be filtered.

To add an entry to the **Access Profile Table**, click the **Add** button. This will open the **Access Profile Configuration** page, as shown below. There are two **Access Profile Configuration** pages – one for **Ethernet** (or MAC address-based) profile configuration, and one for **IP** address-based profile configuration. You can switch between the two **Access Profile Configuration** pages by using the **Type** drop-down menu, and clicking on the **Apply** button. The page shown below is the **IP Access Profile Configuration** page.

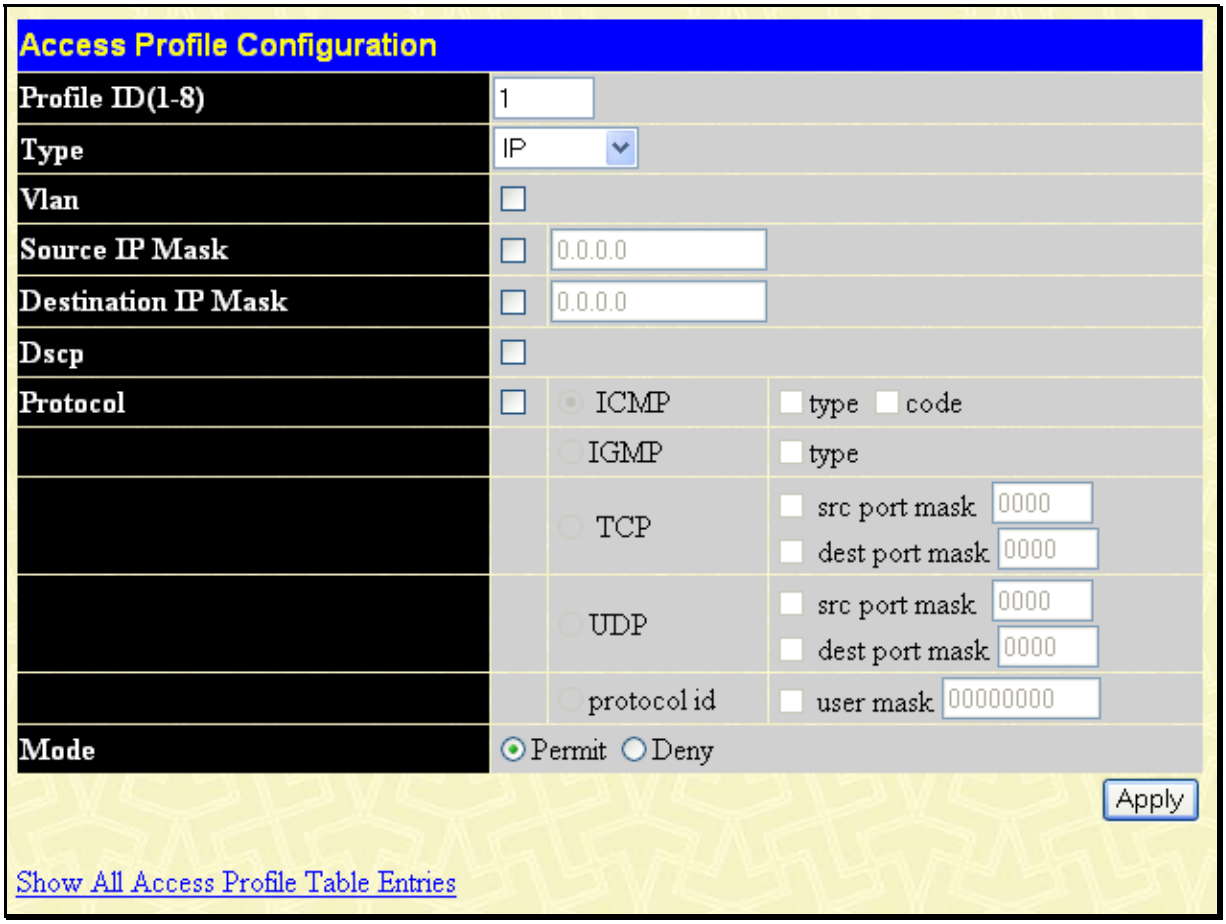


Figure 16-3. Access Profile Configuration (IP)

The following parameters can be set:

Parameter	Description
Profile ID(1-8)	Type in a unique identifier number for this profile set or allow an ID to be automatically assigned by checking the Auto Assign option. This value can be set from 1 – 8.
Type	Select profile based on Ethernet (MAC Address) or IP address. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the switch to examine the layer 2 part of each packet header. Select IP to instruct the switch to examine the IP address in each frame's header.
Vlan	Selecting this option instructs the switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Source IP Mask - Enter an IP address mask for the source IP address.
Destination IP Mask	Destination IP Mask - Enter an IP address mask for the destination MAC address.
Dscp	Selecting this option instructs the switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.

Protocol	Selecting this option instructs the switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines: Select **ICMP** to instruct the switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select **Type** to further specify that the access profile will apply an ICMP type value, or specify **Code** to further specify that the access profile will apply an ICMP cod value. Select **IGMP** to instruct the switch to examine the Internet Group Management Protocol (ICMP) field in each frame's header. Select **Type** to further specify that the access profile will apply an IGMP type value Select **TCP** to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. **src port mask –** Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff). **dest port mask –** Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff). Select **UDP** to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. **src port mask** – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff). **dest port mask** – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff). **protocol id –** Specify a Layer 4 port mask for the destination port in hex form (hex 0x0-0xffffffff).
Mode	Select permit to specify that the packets that match the access profile are forwarded by the switch according to any additional rule added (see below). Select deny to specify that packets that do not match the access profile are not forwarded by the switch and will be filtered.

Section 16

Security IP Management

The Security IP Management page allows you to specify the IP addresses of management stations (PCs) on your network that will be allowed to access the switch's Web-based management agent.

You can enter up to three IP addresses of local hosts (on the same subnet as the switch) that will be allowed to manage the switch. It is recommended that the IP address of the local host that will be used to manage the switch be entered here to avoid possible frequent disconnection from the switch's Web-based management agent.

Go to the **Security Management** folder, click on **Security IP**.

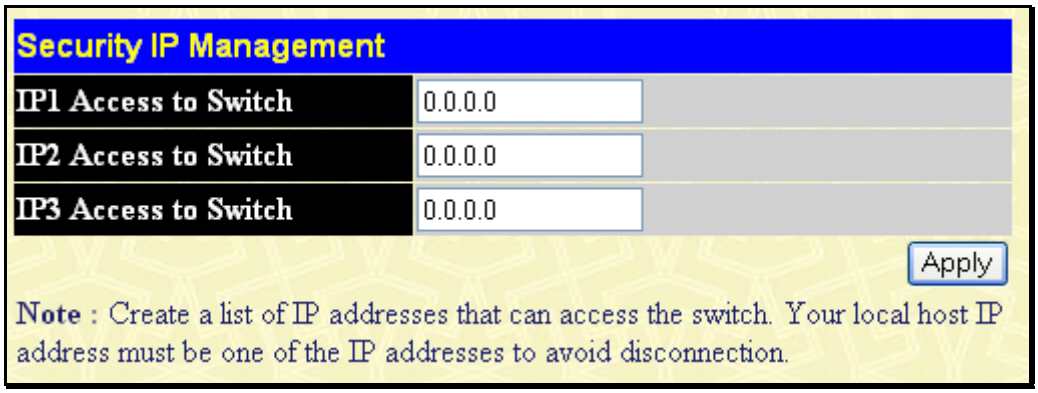


Figure 17-1. Security IP Management

The following fields can be set:

Parameter	Description
IP1 Access to Switch	Enter the IP address of a management station that will be used to manage the switch. This IP address must be on the same subnet as the switch.
IP2 Access to Switch	Enter the IP address of a management station that will be used to manage the switch. This IP address must be on the same subnet as the switch.
IP3 Access to Switch	Enter the IP address of a management station that will be used to manage the switch. This IP address must be on the same subnet as the switch.

Port Access Entity

802.1X Port-based Network Access Control

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

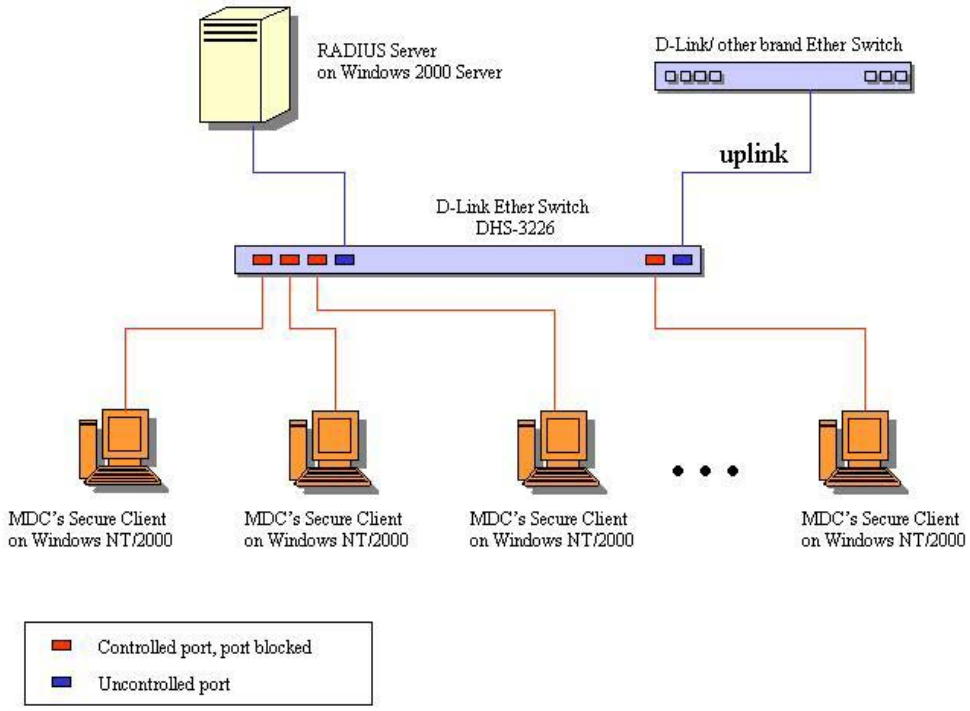


Figure 17-2. Typical 802.1X Configuration Prior to User Authentication

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

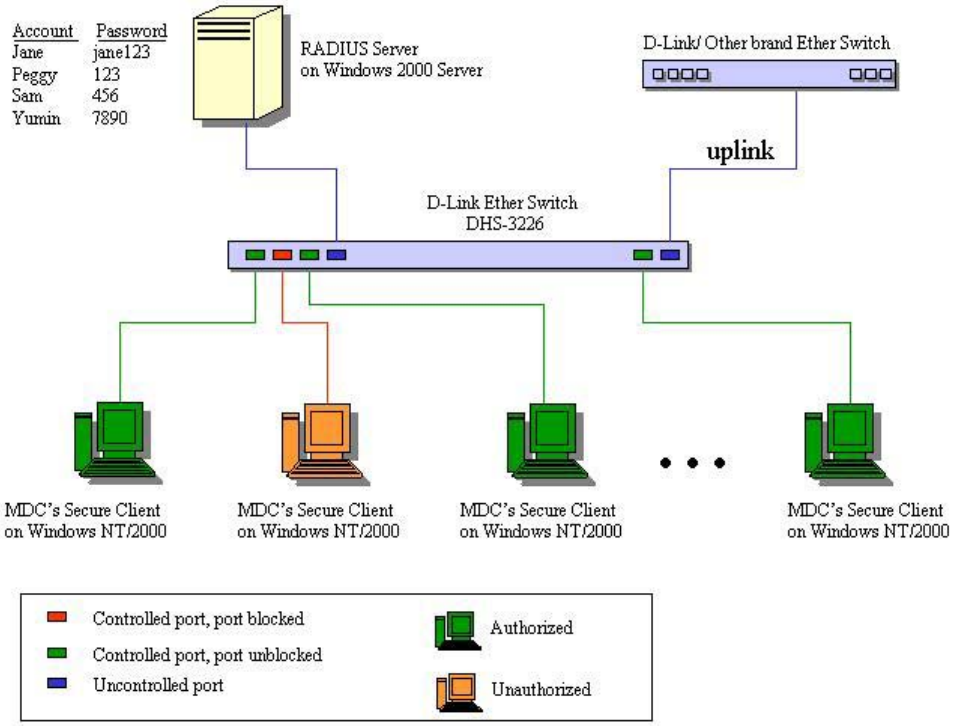


Figure 17-3. Typical 802.1X Configuration with User Authentication

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

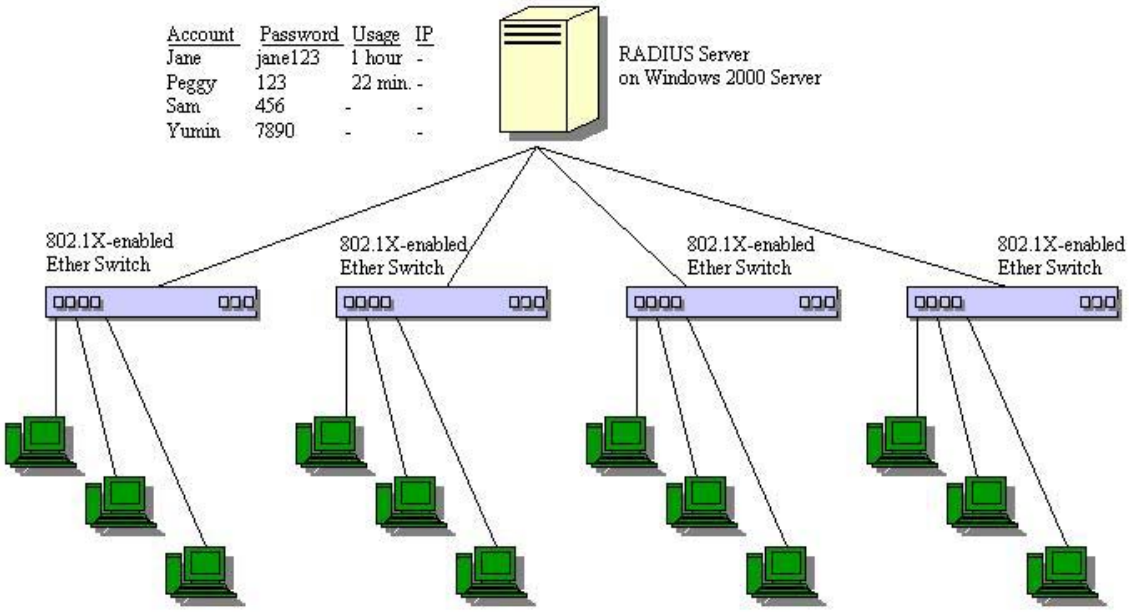


Figure 9 - 1. Typical Configuration with 802.1X Fully Implemented

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

Conformance to IEEE 802.1X Standards

Configure Authenticator

To display the current **802.1X Authenticator Settings** on the switch, open the **Configuration** folder, and then the **Port Access Entity** folder and finally click on the **Configure Authenticator** link. This will open the **802.1X Authenticator Settings** page, as shown below.

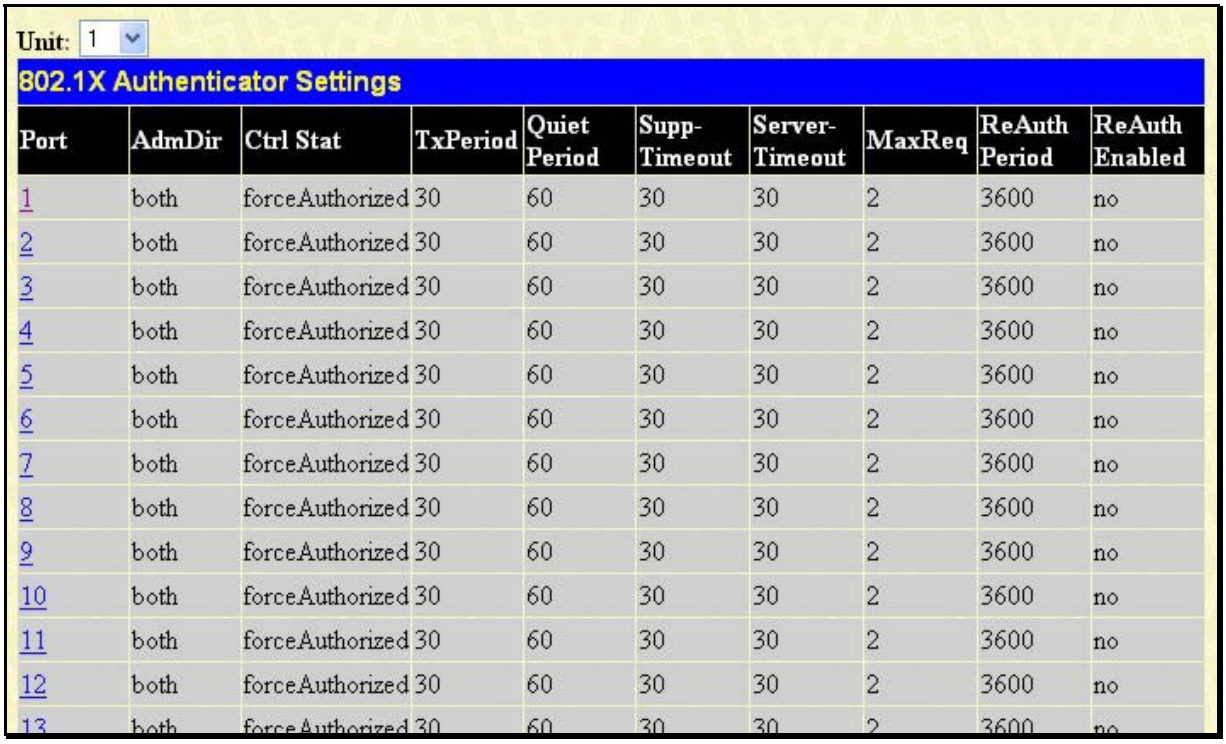


Figure 17-4. 802.1X Authenticator Settings

To configure the 802.1X Authenticator settings for a given port, click on the blue port number under the **Port** heading. This will open the **802.1X Authenticator Settings** page, as shown below.

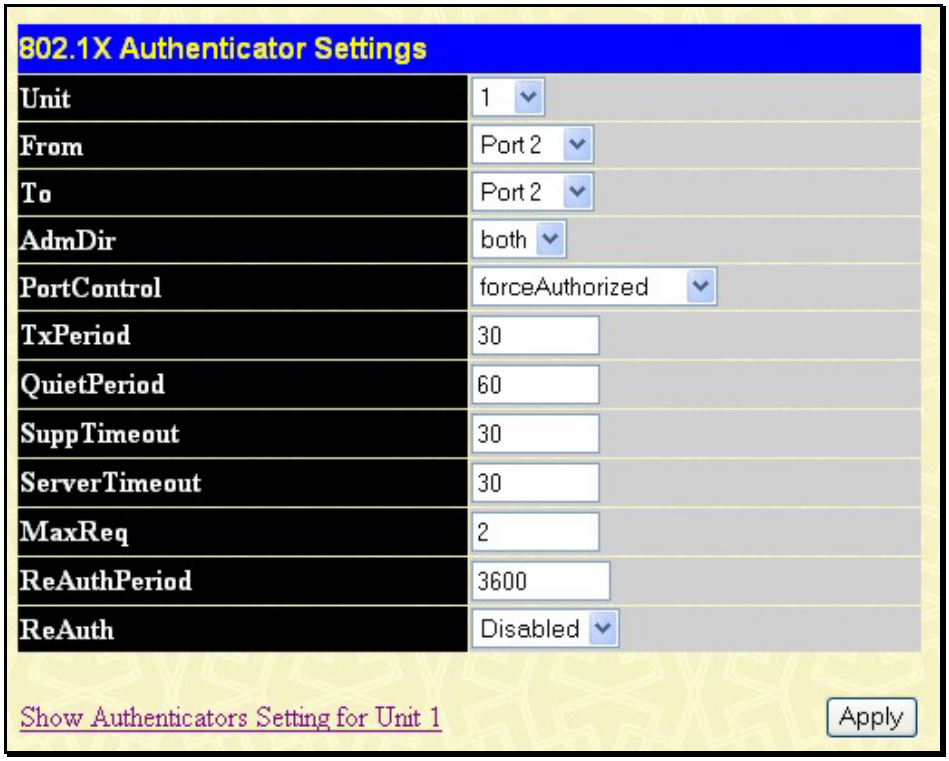


Figure 17-5. 802.1X Authenticator Settings

This window allows you to set the following features:

- **From [ ] To [ ]** – Enter the port or ports to be set.
- **AdmDir [***both***]** – Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
- **PortControl [***auto***]** – This allows you to control the port authorization state. Select *forceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *forceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. The third option is *auto*. This enables 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.
- **TxPeriod [***30* **]** – This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period an EAP Request/Identity packet is transmitted to the client.
- **QuietPeriod [***60* **]** – This allows you to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.
- **SuppTimeout [***30* **]** – This value determines timeout conditions in the exchanges between the Authenticator and the client.
- **ServerTimeout [***30* **]** – This value determines timeout conditions in the exchanges between the Authenticator and the client.
- **MaxReq [***2* **]** – The maximum number of times that the switch will retransmit an EAP Request packet to the client before it times out the authentication session.
- **ReAuthPeriod [***3600* **]** – A constant that defines a nonzero number of seconds between periodic reauthentications of the client.

- **ReAuth [***Disabled***]** – Determines whether regular reauthentication will take place on this port.

The following parameters can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID. 15 indicates a switch in standalone mode.
From/To	A consecutive group of ports may be configured starting with the selected port.
AdmDir	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.
PortControl	From the pull-down menu, select **Force Authorized**, **Force Unauthorized** or **Auto** – **Force Authorized** forces the Authenticator of the port to become Authorized. **Force Unauthorized** forces the port to become Unauthorized.
TxPeriod	Select the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.
QuietPeriod	Select the time interval between authentication failure and the start of a new authentication attempt.
SuppTimeout	Select the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.
ServerTimeout	Select the length of time to wait for a response from a Radius server.
MaxReq	Select the maximum number of times to retry sending packets to the supplicant.
ReAuthPeriod	Select the time interval between successive re-authentications.
ReAuth	Enable or disable reauthentication.

Port Authenticating Settings

To set the port authenticating settings, open the Configuration folder, and then the Port Access Entity folder, and then the PAE System Control folder. Finally click on the Port Authenticating Settings link. This will open the 802.1X Capability Settings page, as shown below.

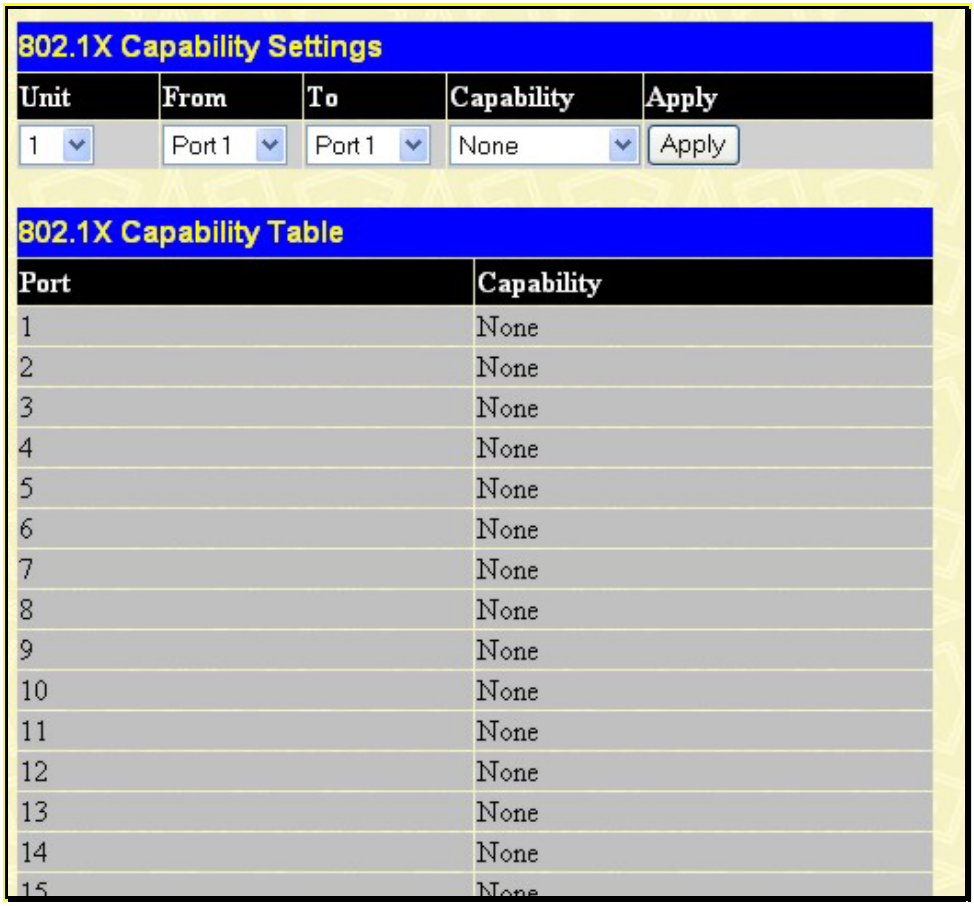


Figure 17-6. 802.1X Authenticator Settings

To set up the Switch's 802.1X port-based authentication, select which ports are to be configured in the **From** and **To** fields. Next, enable the ports by selecting *Authenticator* from the drop-down menu under **Capability**.

Click **Apply** to let your change take effect.

Radius Server

Use this menu to configure the settings the switch will use to communicate with a Radius server. To add Radius server settings click the New button, a separate configuration menu appears. To edit an existing Radius settings index, select it and click the edit button

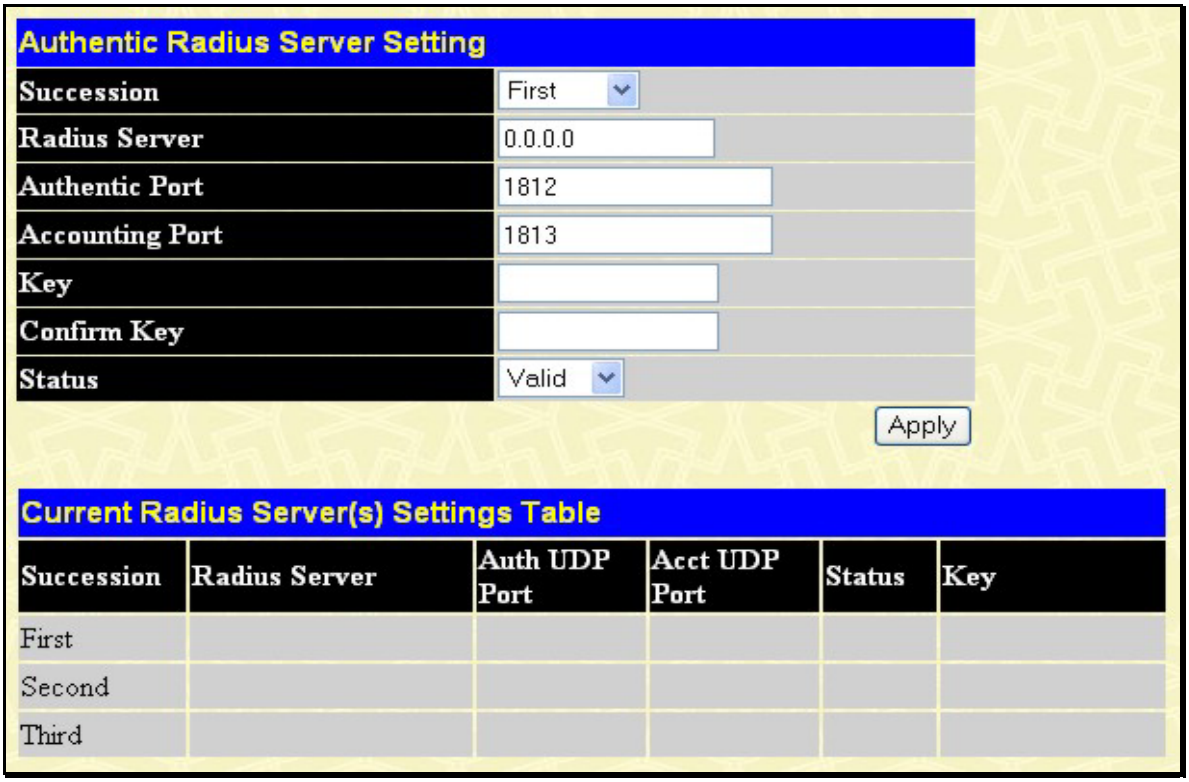


Figure 17-7. 802.1X Authentic Radius Server Setting

The following parameters can be set:

Parameter	Description
Index	Radius server settings index.
Radius Server	Type in the IP address of the Radius server.
Authentic Port	This is the UDP port on the Radius server that will be used to authenticate users. The default is 1812.
Accounting Port	This is the UDP port on the Radius server that will be used to log authentication events. The default is 1813.
Key	Type the shared-secret key used by the Radius server and the switch. Up to 32 characters can be used. Retype the Key in the **Confirm Key** field.
Status	This drop-down menu allows you to select **Valid** or **Invalid**.

Section 17

SNMP

The DGS-3224SR 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 DGS-3224SR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The SNMP version used to monitor and control the switch can be specified by the administrator. 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 User Table

The SNMP User Table displays all of the SNMP Users currently configured on the switch.

Open the **SNMP Manager** folder and then the **SNMP User Table** link.

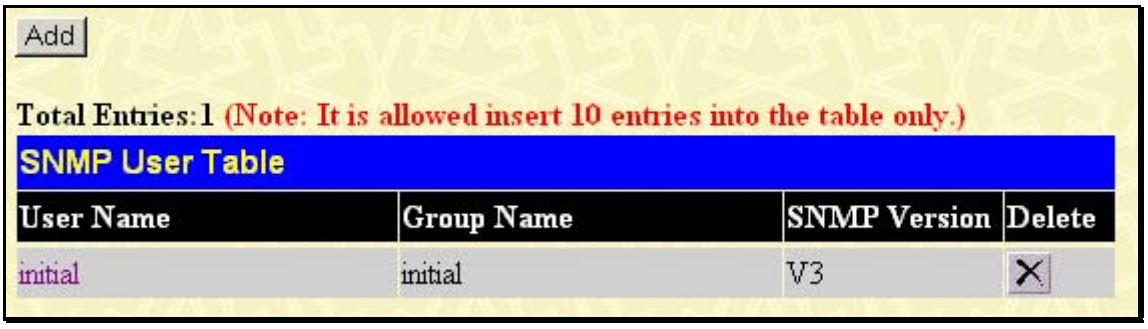


Figure 18-1. SNMP User Table

To delete an existing SNMP User Table entry, click on the **X** icon below the **Delete** heading corresponding to the entry you want to delete.

To display the detailed entry for a given user, click on the blue **User Name**. This will open the **SNMP User Table Display** page, as shown below.

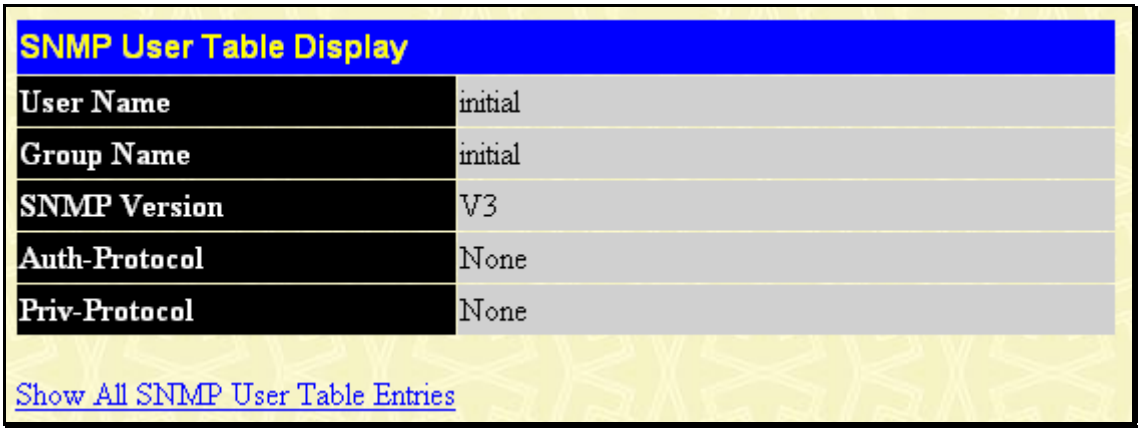


Figure 18-2. SNMP User Table Display

The following parameters are displayed:

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 can request SNMP messages.
SNMP Version	**V1** – Indicates that SNMP version 1 will be used. **V2** – Indicates that SNMP version 2 will be used. **V3** – Indicates that SNMP version 3 will be used.
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.

To add a new entry to the **SNMP User Table Configuration**, click on the Add button on the **SNMP User Table** page. This will open the **SNMP User Table Configuration** page, as shown below.

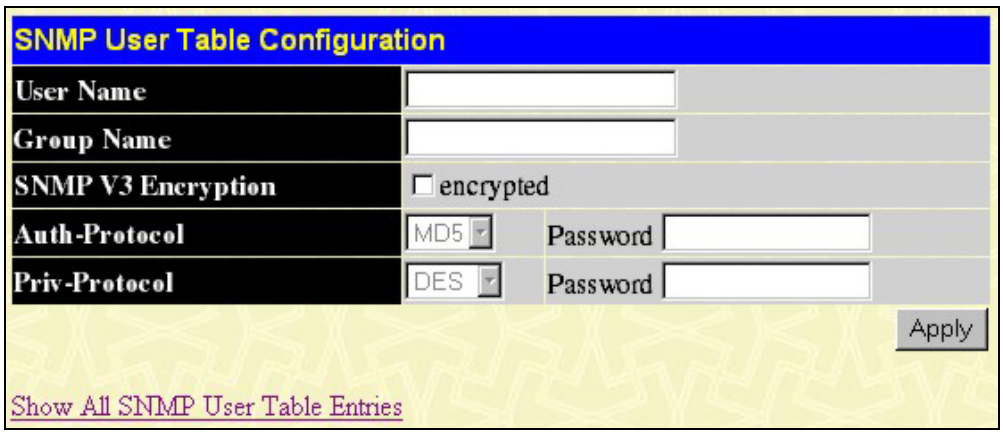


Figure 18-3. SNMP User Table Configuration

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 can request SNMP messages.
SNMP Version	**V1** – Specifies that SNMP version 1 will be used. **V2c** – Specifies that SNMP version 2c will be used. **V3** – Specifies that SNMP version 3 will be used.
Auth-Protocol	**None** – Specifies that no authorization protocol is in use. **MD5** – Specifies that the HMAC-MD5-96 authentication level will be used. **SHA** – Specifies that the HMAC-SHA authentication protocol will be used.
Priv-Protocol	**None** – Specifies that no authorization protocol is in use. **DES** – Specifies that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

SNMP View Table

The **SNMP View Table** is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager.

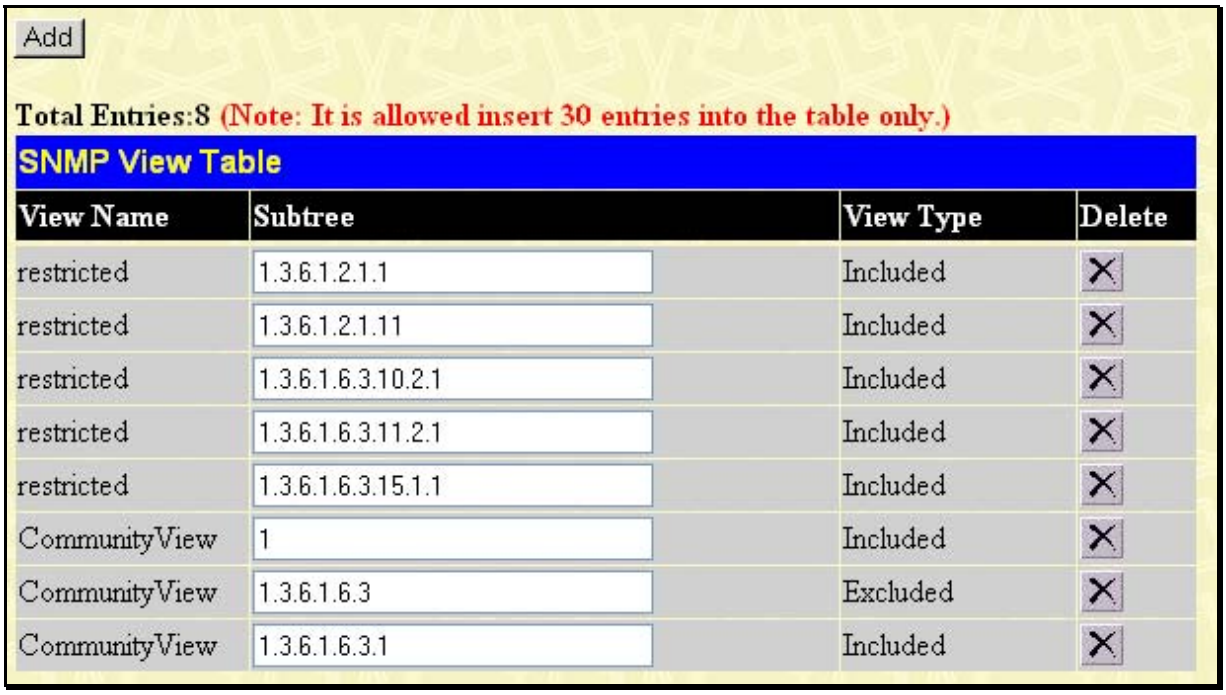


Figure 18-4. SNMP View Table

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 **Add** button, a separate menu will appear.

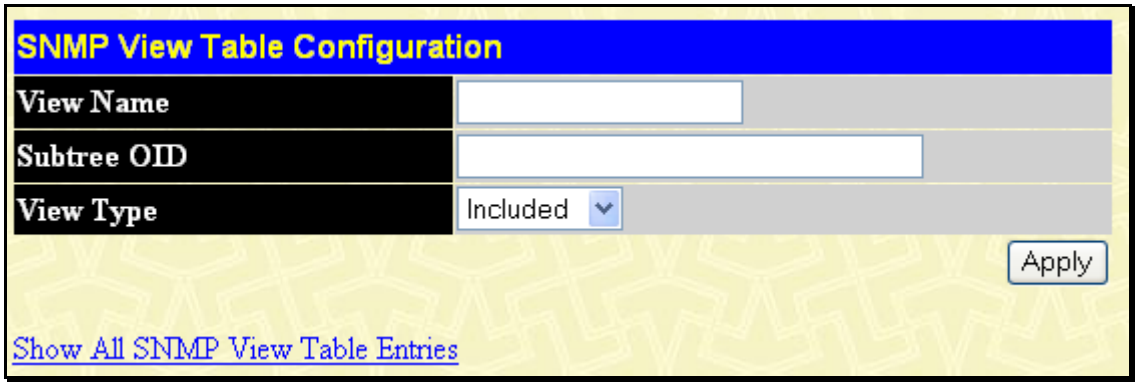


Figure 18-5. SNMP View Table Configuration

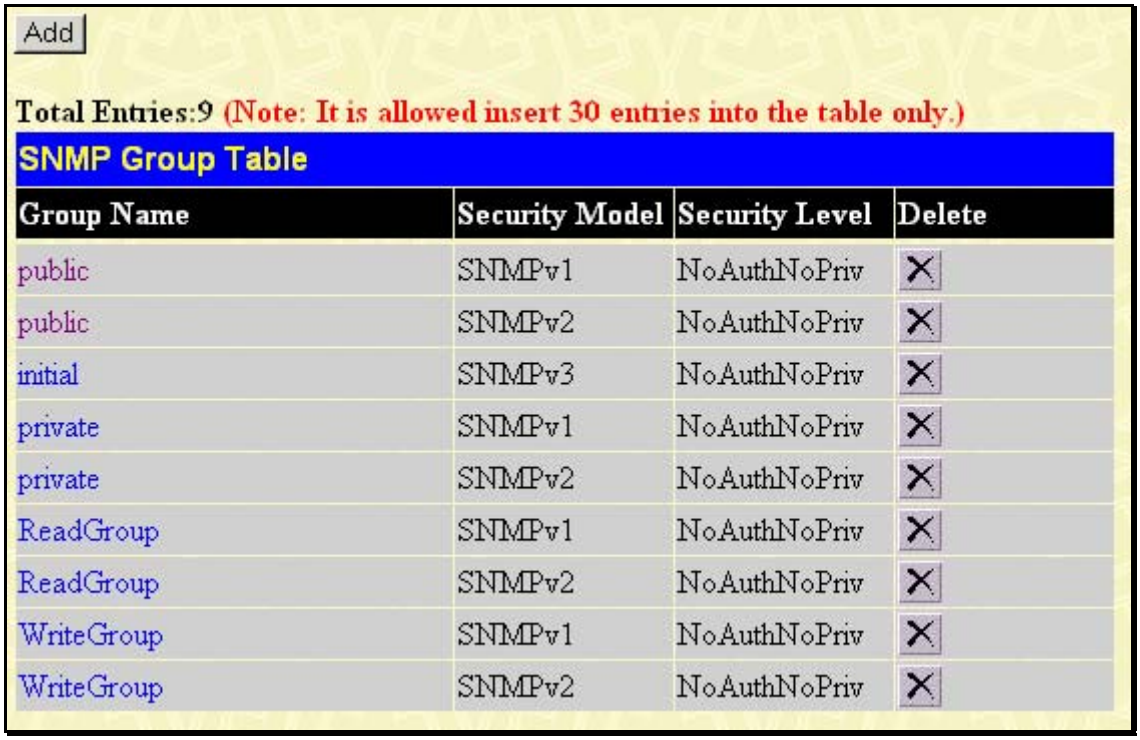
The SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table**) to the views created in the previous menu.

The following parameters can 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.



Add

Total Entries:9 (Note: It is allowed insert 30 entries into the table only.)

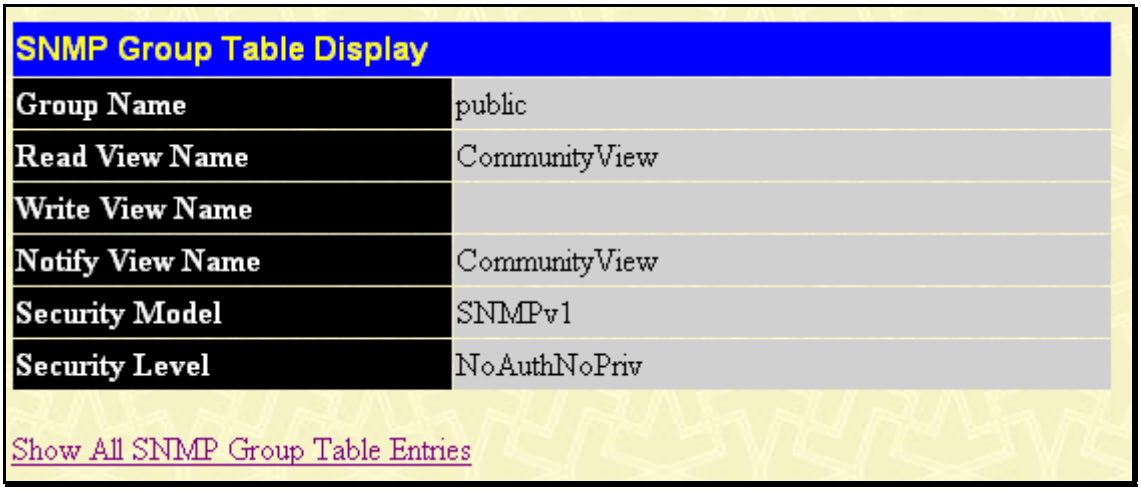
SNMP Group Table

Group Name	Security Model	Security Level	Delete
public	SNMPv1	NoAuthNoPriv	X
public	SNMPv2	NoAuthNoPriv	X
initial	SNMPv3	NoAuthNoPriv	X
private	SNMPv1	NoAuthNoPriv	X
private	SNMPv2	NoAuthNoPriv	X
ReadGroup	SNMPv1	NoAuthNoPriv	X
ReadGroup	SNMPv2	NoAuthNoPriv	X
WriteGroup	SNMPv1	NoAuthNoPriv	X
WriteGroup	SNMPv2	NoAuthNoPriv	X

Figure 18-6. SNMP Group Table

To delete an existing SNMP Group Table entry, click the corresponding **X** icon under the **Delete** heading.

To display the current settings for an existing SNMP Group Table entry, click the blue link for the entry under the **Group Name** heading.



SNMP Group Table Display

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

Show All SNMP Group Table Entries

Figure 18-7. SNMP Group Table Display

To add a new entry to the switch's SNMP Group Table, click the Add 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.

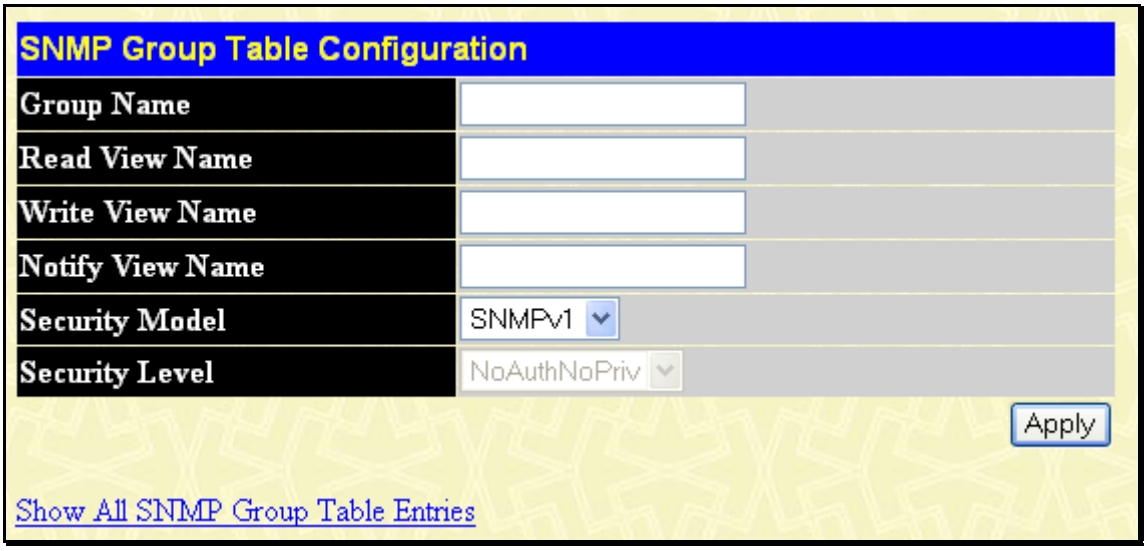


Figure 18-8. SNMP Group Table Configuration

The following parameters can set:

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 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.

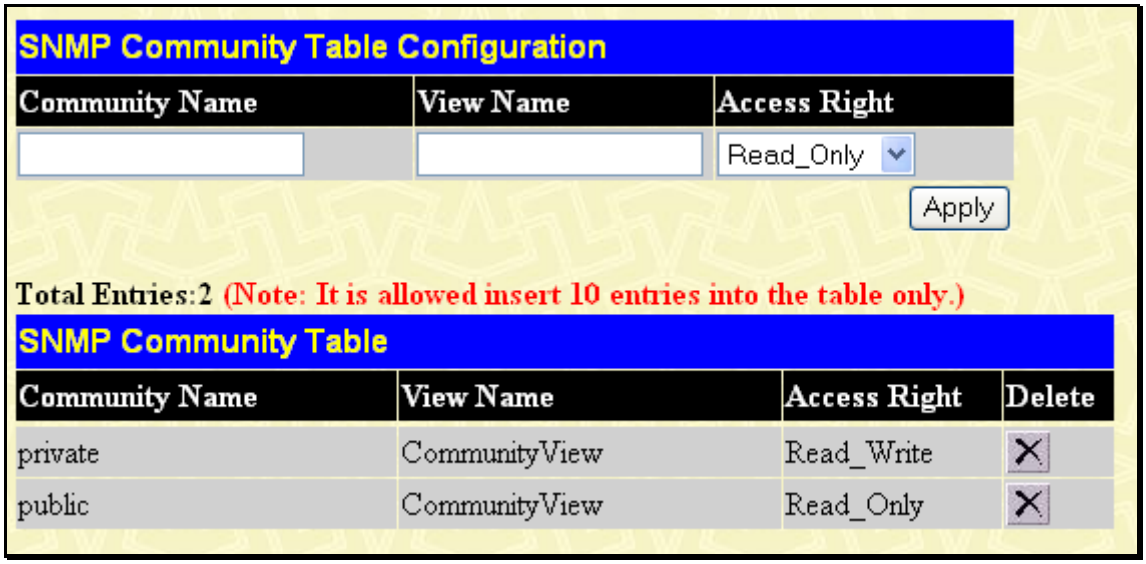


Figure 18-9. SNMP Community Table Configuration

The following parameters can set:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 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 **Management** folder, 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 **X** icon under the **Delete** heading.

To display the current settings for an existing SNMP Group Table entry, click the blue link for the entry under the **Host IP Address** heading.

Figure 18-10. SNMP Host Table

To add a new entry to the switch's SNMP Group Table, click the Add 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.

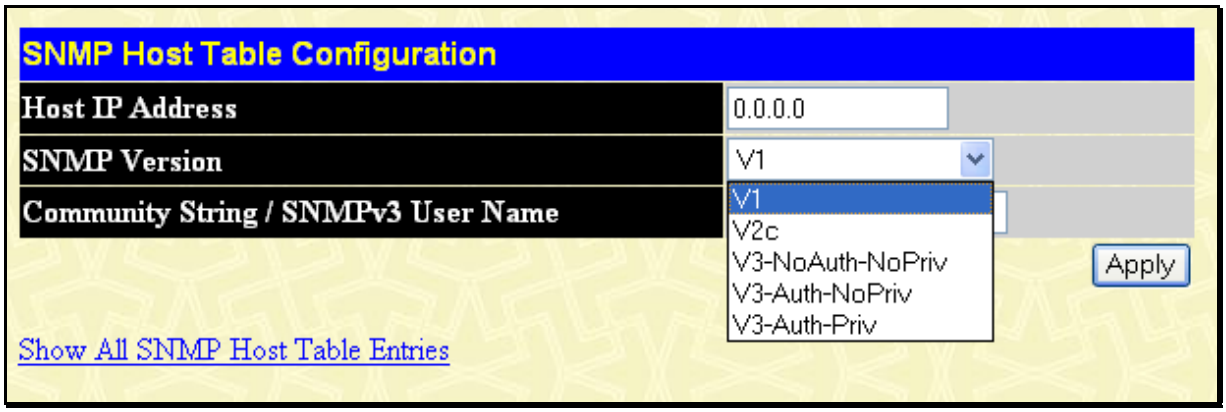


Figure 18-11. SNMP Host Table Configuration

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 version 2 will be used. **V3** – To specify that the SNMP version 3 will be used. (Qualifiers denote administrative status.)
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 **SNMP Manager** folder and click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID** Configuration window, as shown below.

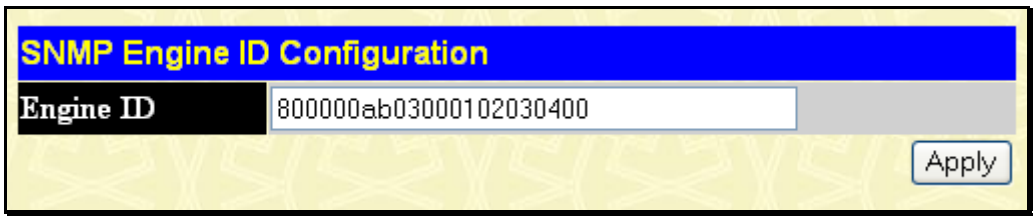


Figure 18-12. SNMP Engine ID Configuration

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

Section 18

System Monitoring and Statistics

The DGS-3224SR provides extensive network monitoring capabilities that can be viewed from the **Monitoring** folder.

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 a line graph or table format.

To view the port utilization, click on the **Monitoring** folder and then the **Port Utilization** link:

Figure 19-1. Port Utilization Line Chart

The following field can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID. 15 indicates a switch in standalone mode.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.

Packets

Received Packets

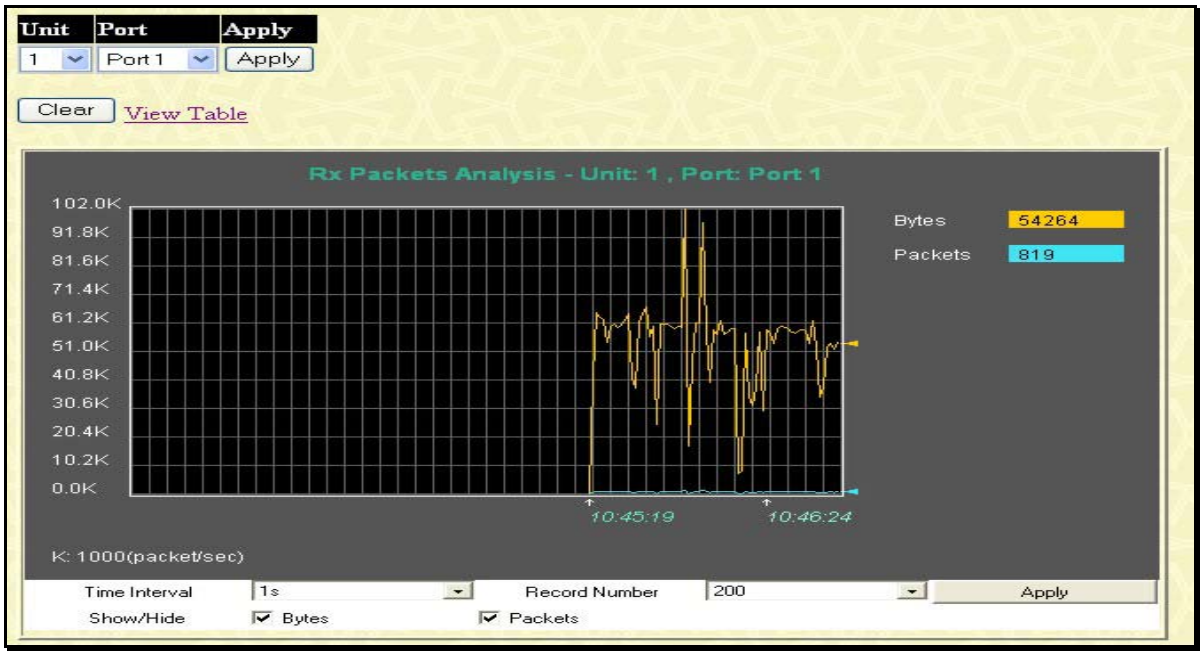
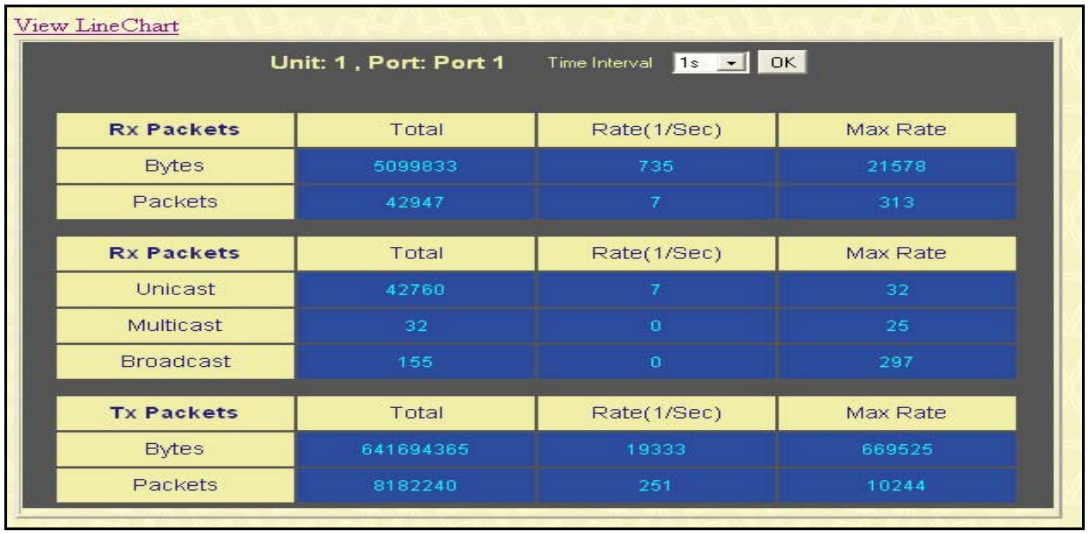


Figure 19-2. Rx Packets Line Chart

Select the desired switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated.

The following fields can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.



Received Unicast/Multicast/Broadcast Packets

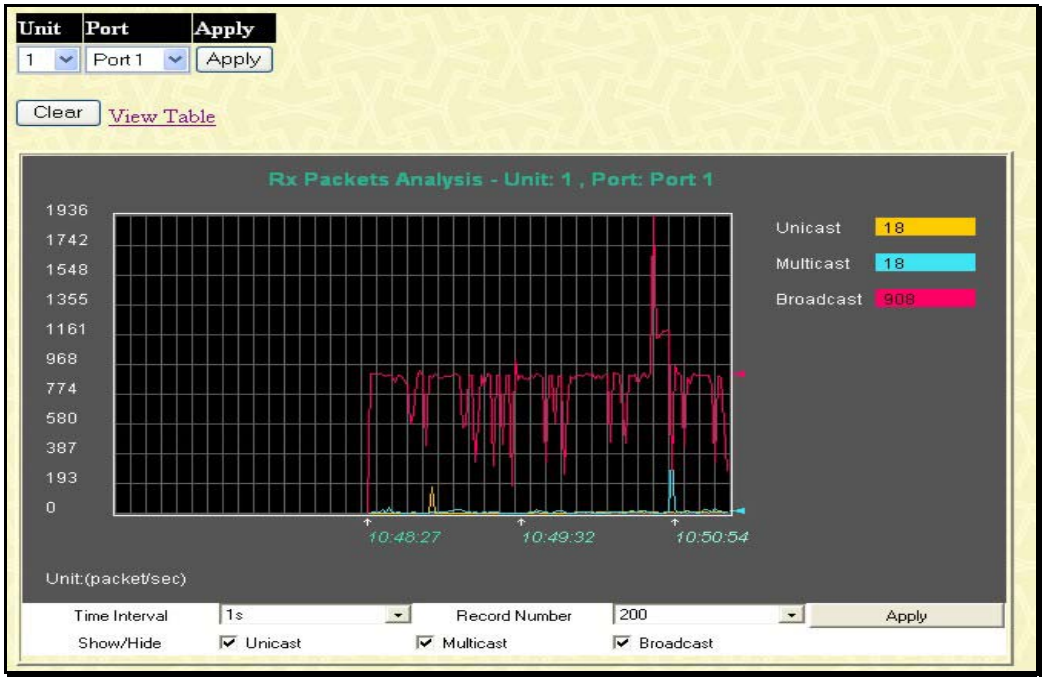


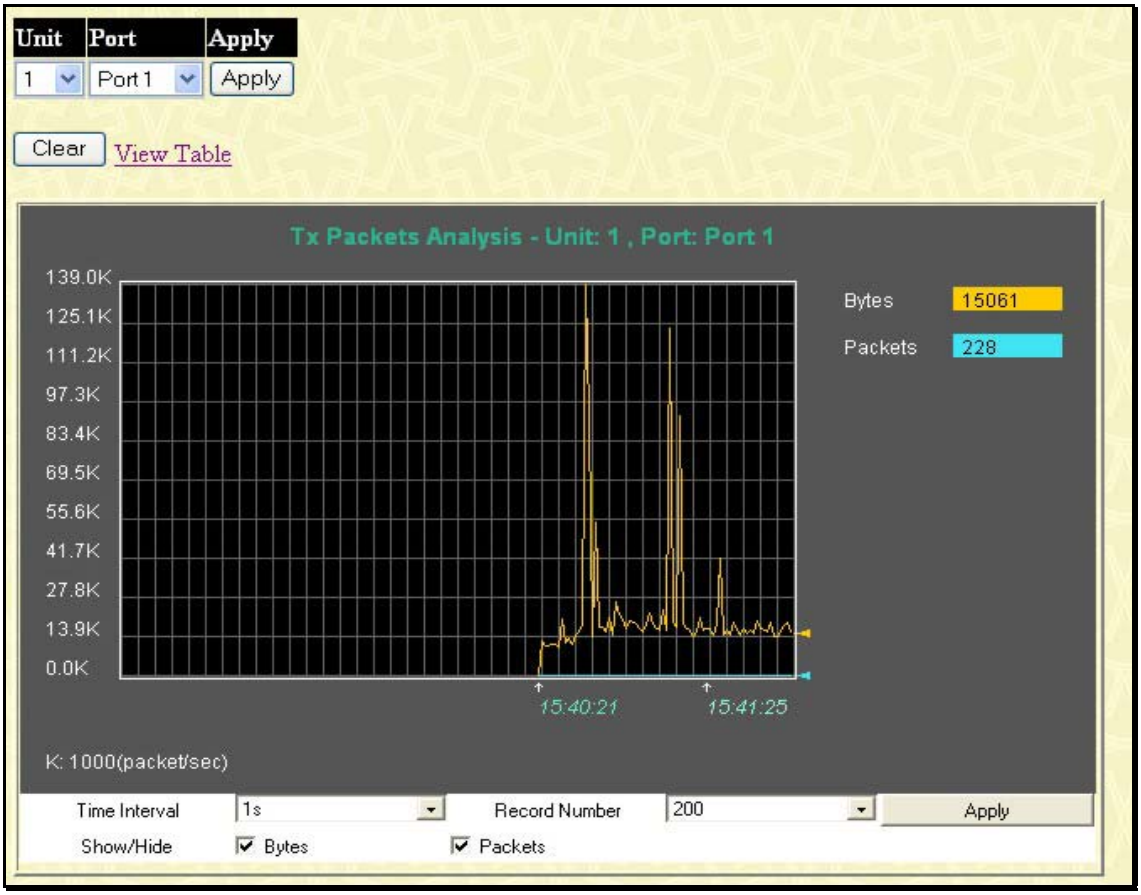
Figure 19-3. Rx Packets UMB Line Chart

Select the desired switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated.

The following field can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.

Transmitted Packets



Select the desired switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated.

The following field can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.

Errors

Transmitted Errors

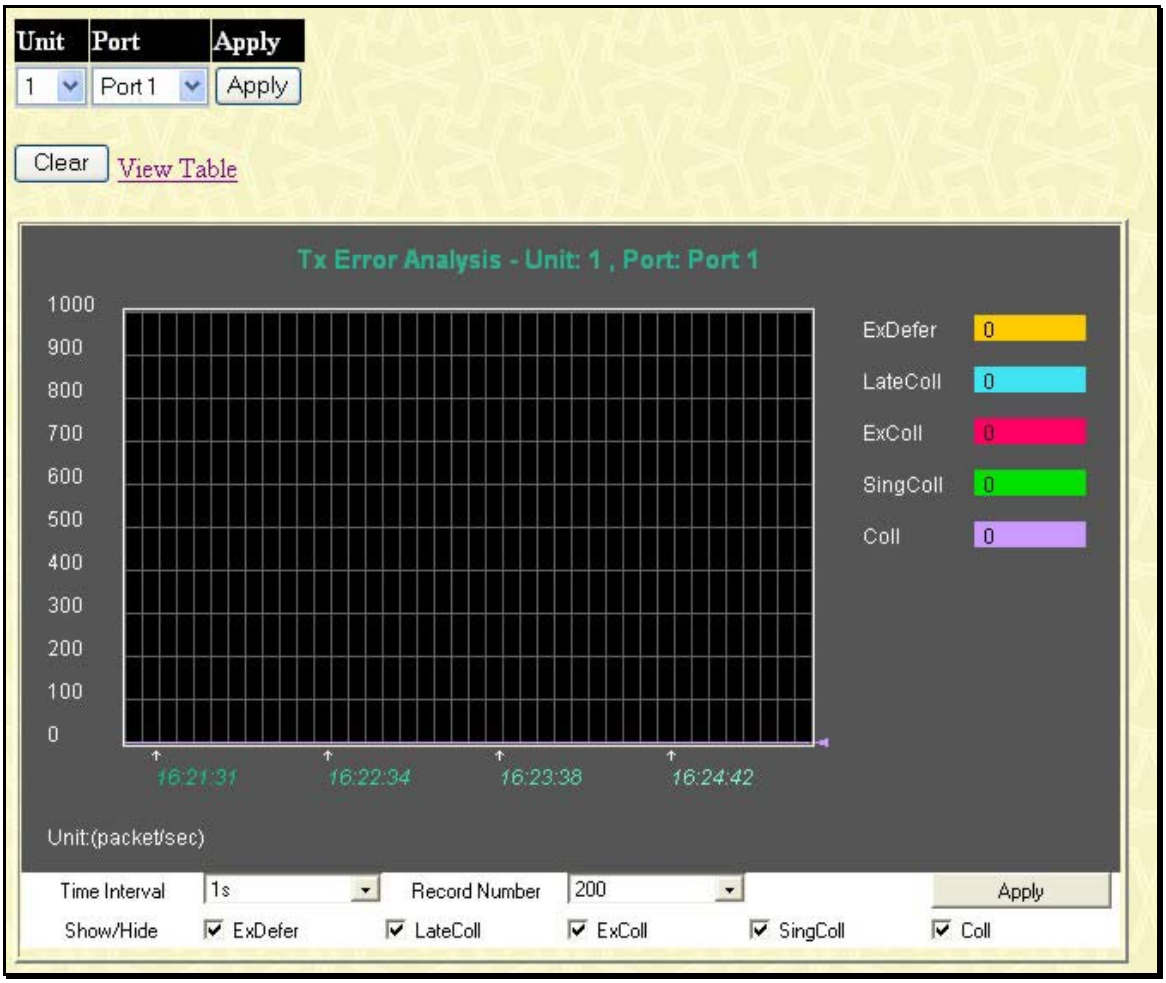


Figure 19-4. Transmitted Error Packets Line Chart

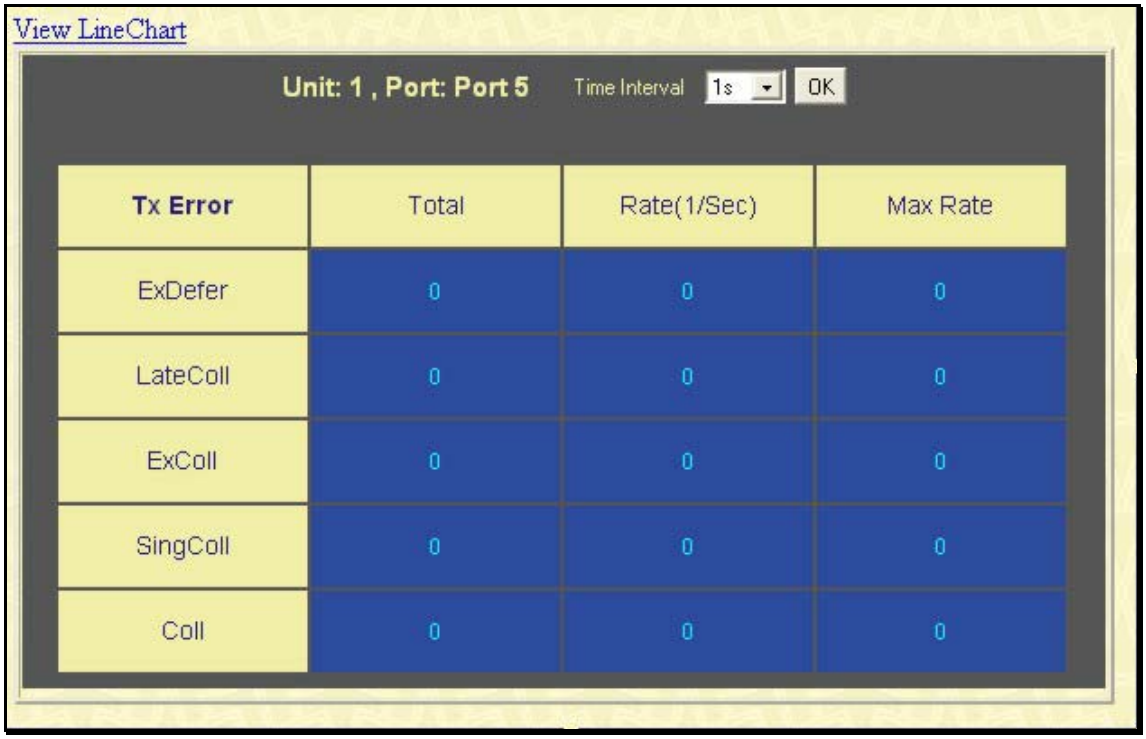
Select the desired switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated.

The following field can be set or are displayed:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID. 15 indicates a switch in standalone mode.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.
ExDefer (Excessive Deferral)	The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.

LateColl (Late Collision)	Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl (Excessive Collision)	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.
SingColl (Single Collision)	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
Coll (Collision)	An estimate of the total number of collisions on this network segment.

Click **View Table** to view the same information in tabular form.



Received Errors

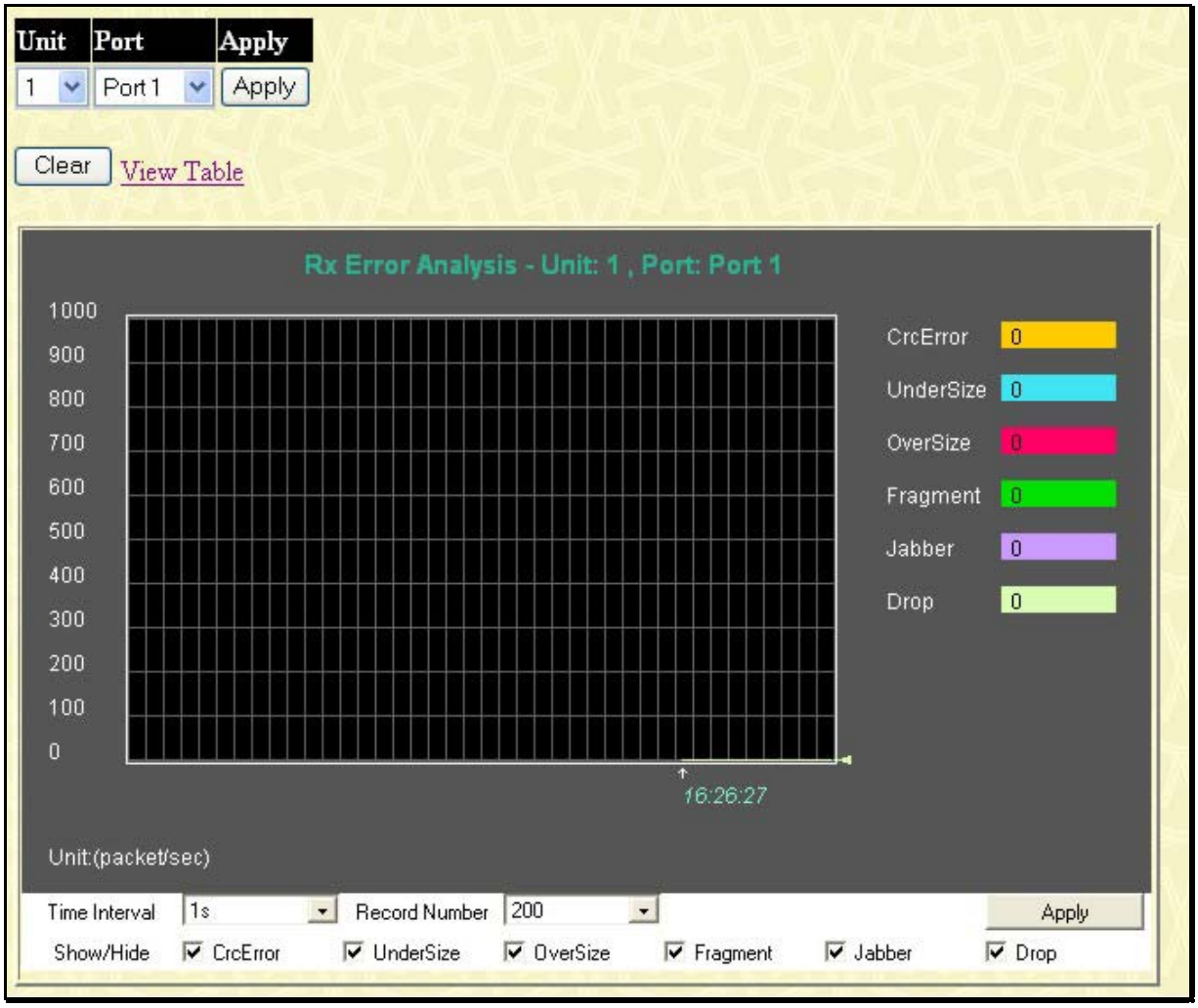


Figure 19-5. Rx Error Packets Line Chart

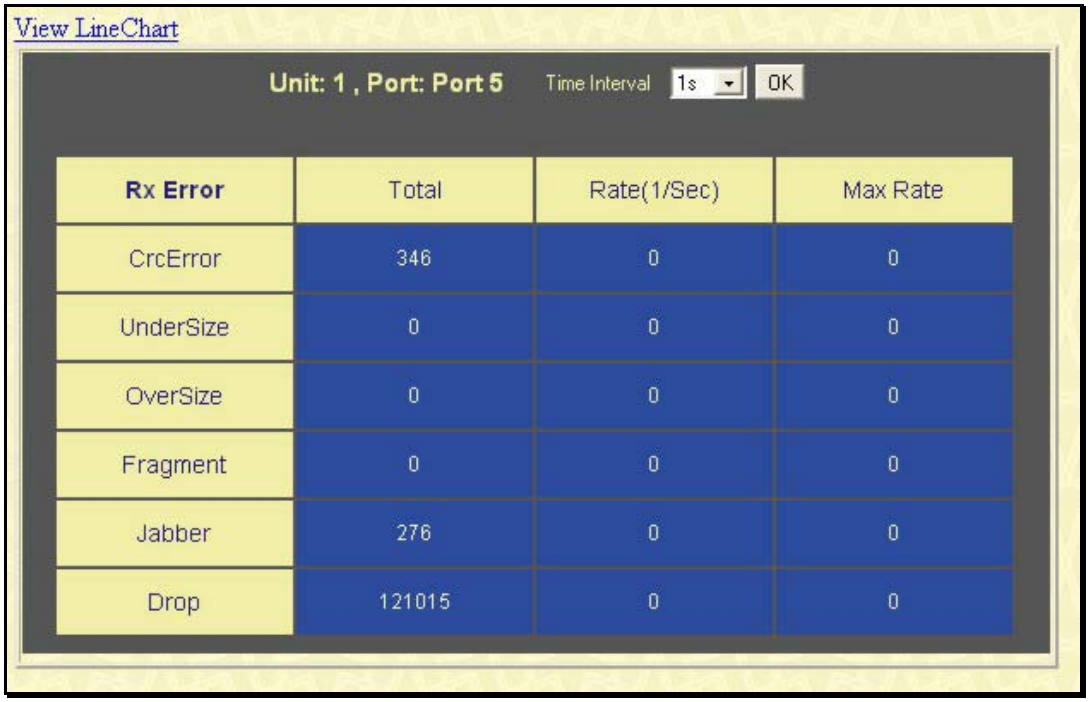
Select the desired switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated.

The following field can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID. 15 indicates a switch in standalone mode.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.
CrcError	For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
UnderSize	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well

	formed.
OverSize	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragment	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or an alignment error.
Jabber	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or an alignment error.
Drop	The total number of events in which packets were dropped due to a lack of resources.

Click **View Table** to see the same information in tabular form.



Size

Packet Size

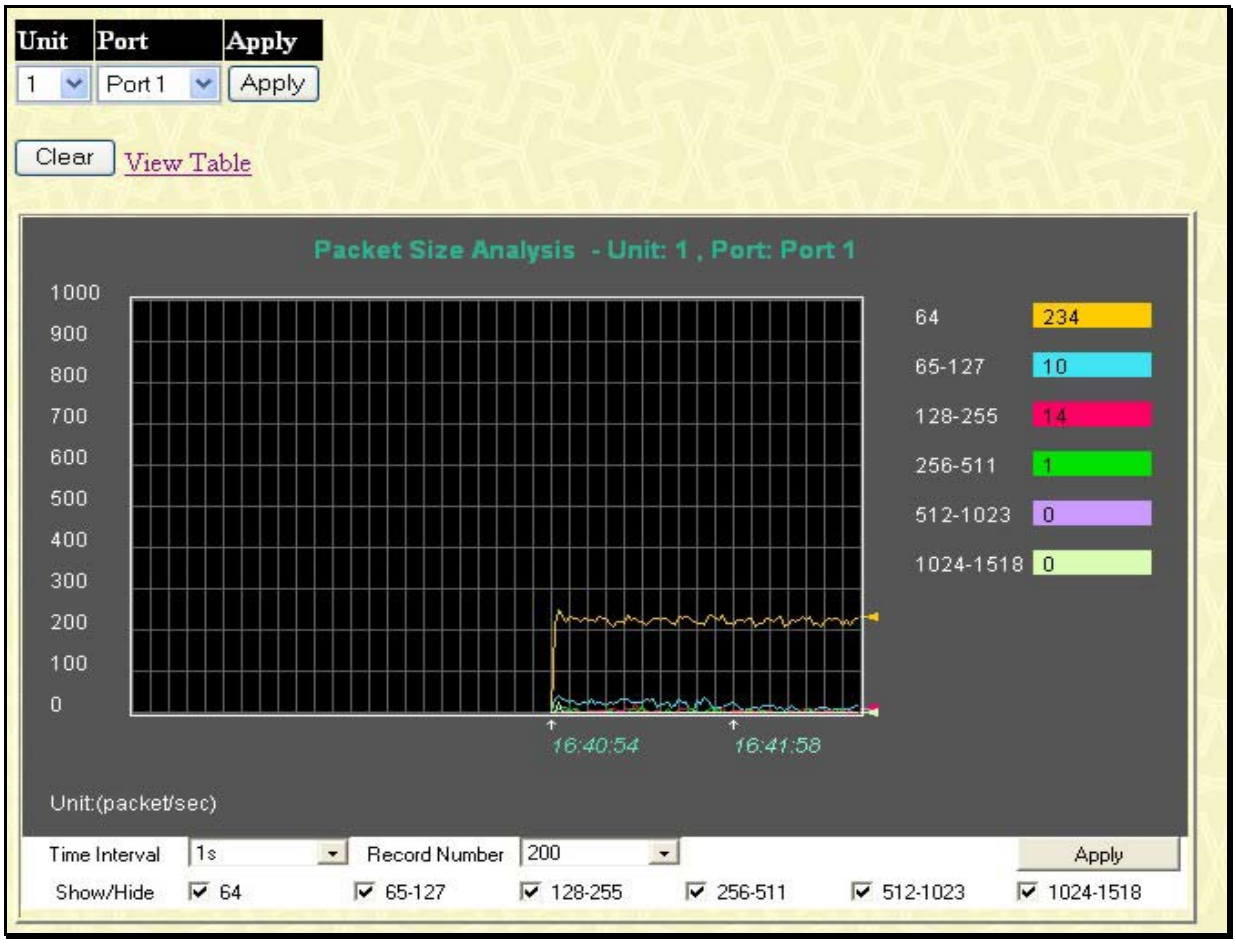


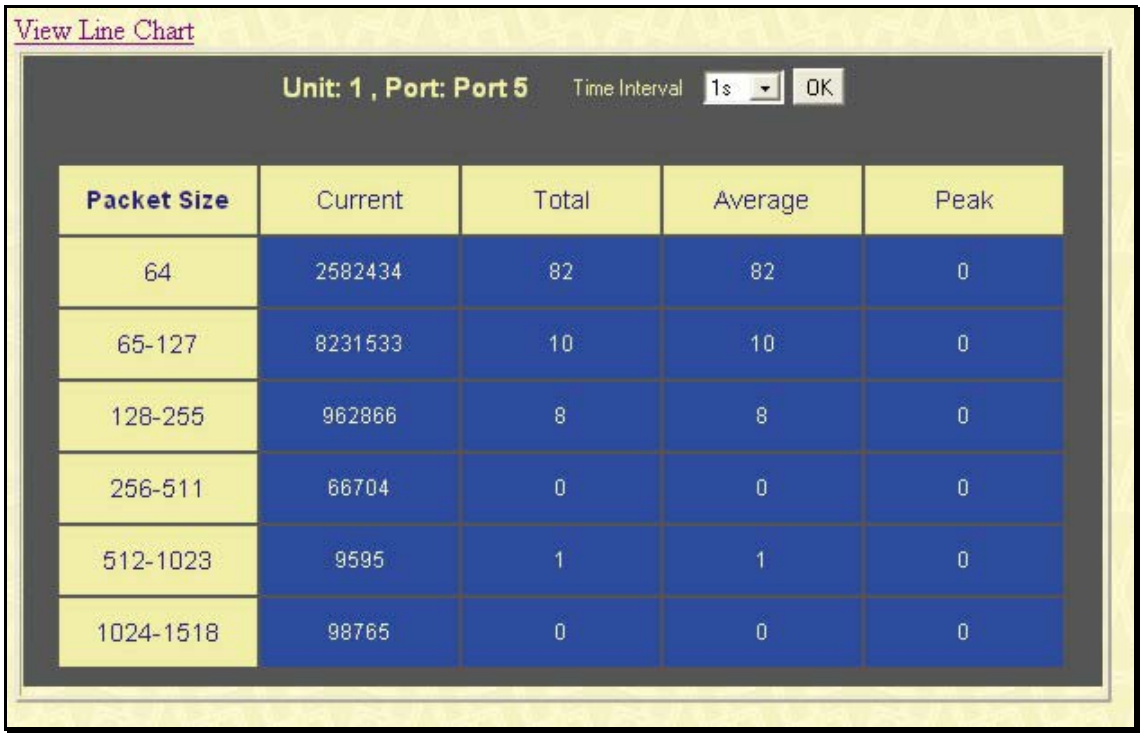
Figure 19-6. Packet Size Analysis Line Chart

Select the desired switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated.

The following fields can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID. 15 indicates a switch in standalone mode.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.

Click **View Table** to see the same information in tabular form.



MAC Address

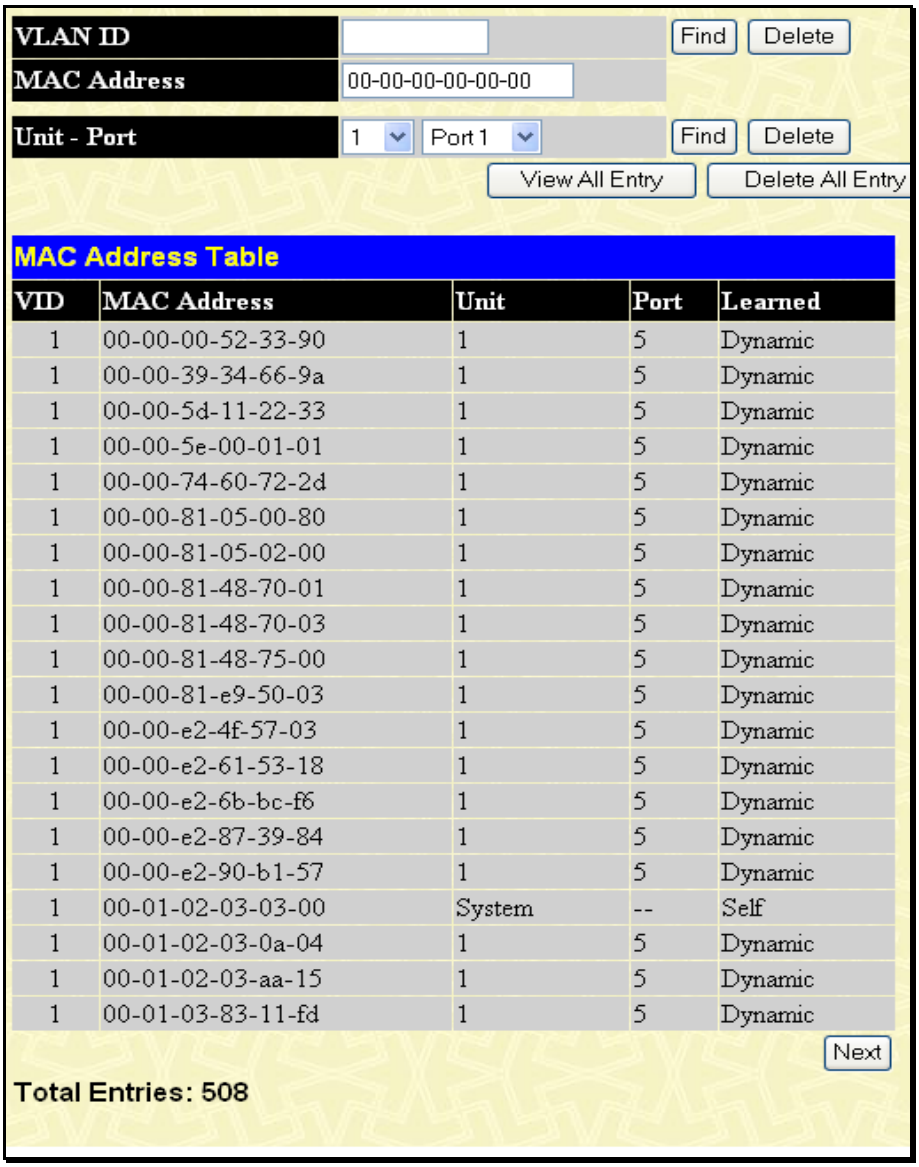


Figure 19-7. MAC Address Table

Select the desired switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Update Interval** field sets the interval at which the error statistics are updated.

The following fields can be set:

Parameter	Description
Unit	Allows you to specify a switch in a switch stack using that switch's Unit ID.
Port	Allows you to specify a port to monitor – from the switch selected above.
Update Interval	The time between updates received from the switch, in seconds. **Suspend** stops the updates. The default is **1s**.

Switch History

Switch History

Sequence	Time	Log Text
122	000d00h46m	Successful login through Web (Username: bob)
121	000d00h00m	Unit 1, System started up
120	000d00h00m	Port 1:9 link up, 100Mbps FULL duplex
119	000d00h00m	Port 1:5 link up, 100Mbps FULL duplex
118	000d00h00m	Port 1:1 link up, 100Mbps FULL duplex
117	000d00h05m	Unit 1, Configuration saved to flash (Username: bob)
116	000d00h01m	Unit 2, Login failed through Console (Username: Anonymous)
115	000d00h01m	Unit 2, Login failed through Console (Username: Anonymous)
114	000d00h01m	Unit 2, Console session timed out (Username: Anonymous)
113	000d00h01m	Unit 2, Logout through Console (Username: Anonymous)
112	000d00h00m	Unit 1, Successful login through Console (Username: bob)
111	000d00h00m	Unit 1, Login failed through Console (Username: Anonymous)
110	000d00h00m	Unit 1, Login failed through Console (Username: Anonymous)
109	000d00h00m	Unit 1, Login failed through Console (Username: Anonymous)
108	000d00h00m	Unit 1, System started up
107	000d00h00m	Port 1:9 link up, 100Mbps FULL duplex
106	000d00h00m	Port 1:5 link up, 100Mbps FULL duplex
105	000d00h00m	Port 1:1 link up, 100Mbps FULL duplex
104	000d02h18m	Unit 1, Configuration saved to flash (Username: bob)
103	000d02h16m	Unit 1, Successful login through Console (Username: bob)

Clear Next

Figure 19-8. Switch History

IGMP Snooping

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 number of IGMP reports that were snooped is also displayed in the **Reports** field.

Total Entries : 1

IGMP Snooping Table

VLAN ID	Multicast Group	MAC Address	Queries	Reports
0	0.0.0.0	00:00:00:00:00:00	Disabled	0

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

Figure 19-9. IGMP Snooping Table

The following fields can be set:

Parameter	Description
Multicast Group	The IP address of the multicast group.
MAC Address	The MAC address of the multicast group.
Reports	The total number of reports received for this group.

Browse Router Port

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**.

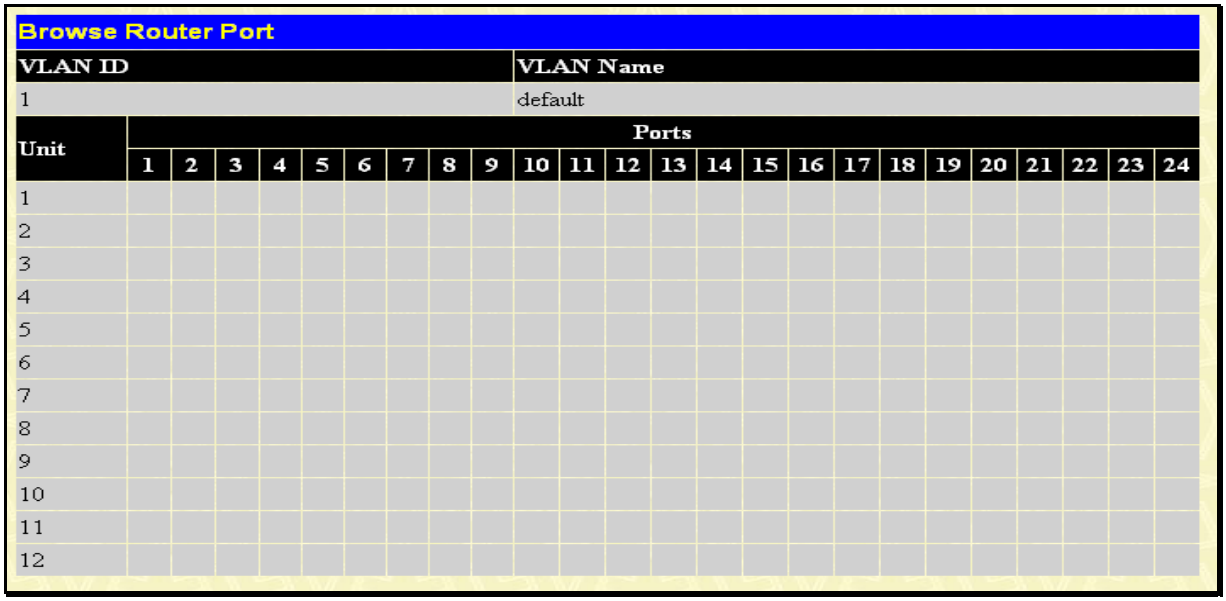


Figure 19-10. Browse Router Port

Section 19

Maintenance

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

To update the switch's firmware, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Download Firmware** link:

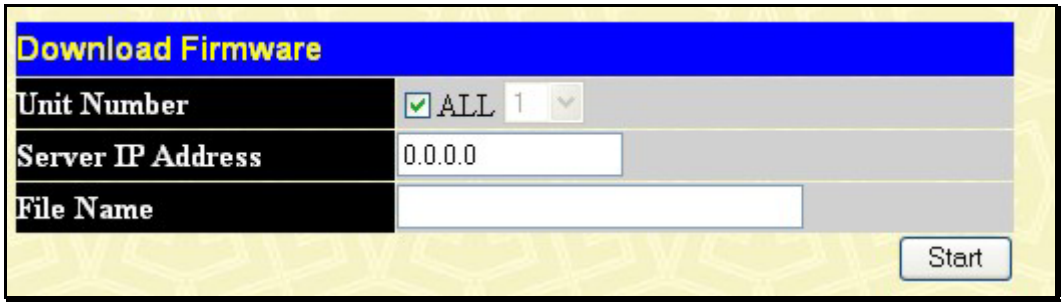


Figure 20-1. Download Firmware

Unit ID – Select which switch of a switch stack you want to update the firmware on. This allows the selection of a particular switch from a switch stack if you have installed the optional stacking module and have properly interconnected the switches. 15 indicates a switch in standalone mode.

Enter the IP address of the TFTP server in the **Server IP Address** field.

The TFTP server must be on the same IP subnet as the switch.

Enter the path and the filename to the firmware file on the TFTP server.

The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages – such as NetSight, or can be obtained as a separate program.

Click **Start** to record the IP address of the TFTP server.

Download Configuration File

To download a configuration file from a TFTP server, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Download Configuration File** link:

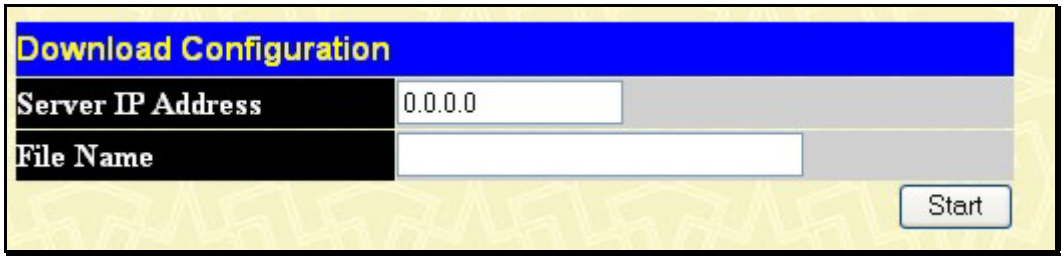


Figure 20-2. Download Configuration

Enter the IP address of the TFTP server and specify the location of the switch configuration file on the TFTP server.

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

Upload Configuration

To upload the switch settings to a TFTP server, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Upload Configuration** link:

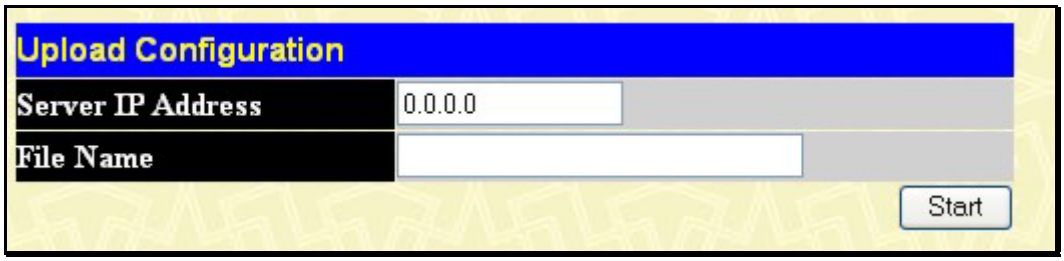


Figure 20-3. Save Settings to TFTP Server

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server.

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

Upload Log

To upload the switch history log file to a TFTP server, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Upload Log** link:

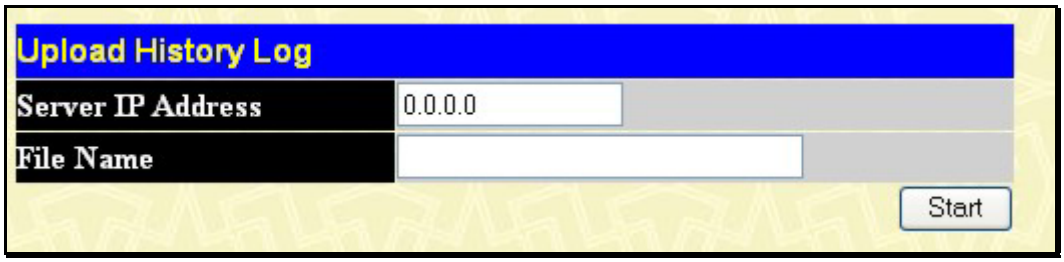


Figure 20-4. Save Switch History to TFTP Server

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server.

Click **Start** 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.

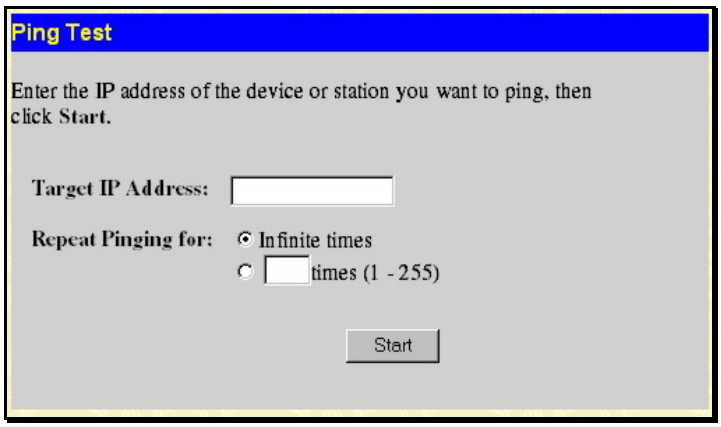


Figure 20-5. Ping Test

The **Infinite times** checkbox, in the **Number of Repetitions** field, tells ping to keep sending data packets to the specified IP address until the program is stopped.

Save Changes

The DGS-3224SR has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective clicking the **Apply** button**.** When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

Some settings, though, require you to restart the switch before they will take effect. Restarting the switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

To retain any configuration changes permanently, click on the **Save Configuration** button in the **Save Changes** page, as shown below.

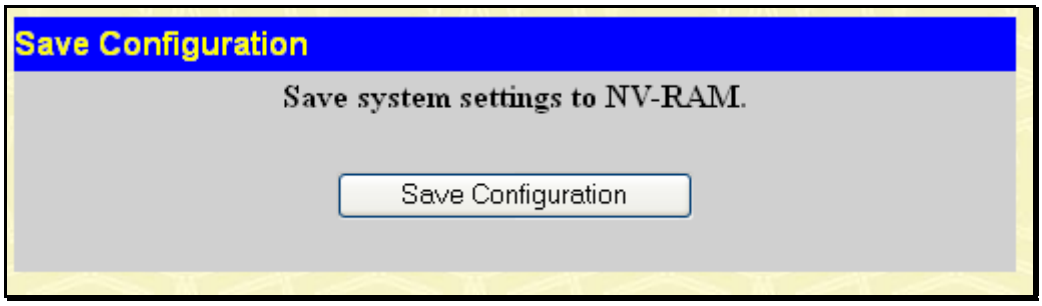


Figure 20-6. Save Changes

Once the switch configuration settings have been saved to NV-RAM, they become the default settings for the switch. These settings will be used every time the switch is rebooted.

Factory Reset

The **Factory Reset** function has several options when resetting the switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

Note: only the **Reset System** option will enter the factory default parameters into the switch's non-volatile RAM, and then restart the switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. **Reset System** will return the switch's configuration to the state it was when it left the factory.

Reset gives the option of retaining the switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the switch is reset with this option enabled, and **Save Changes** is not executed, the switch will return to the last saved configuration when rebooted.

The **Reset Config** option will reset all of the switch's configuration parameters to their factory defaults, without saving these default values to the switch's non-volatile RAM. If the switch is reset with this option enabled, and **Save Changes** is not executed, the switch will return to the last saved configuration when rebooted.

In addition, the **Reset System** option is added to reset all configuration parameters to their factory defaults, save these parameters to the switch's non-volatile RAM, and then restart the switch. This option is equivalent to **Reset Config** (above) followed by **Save Changes**.

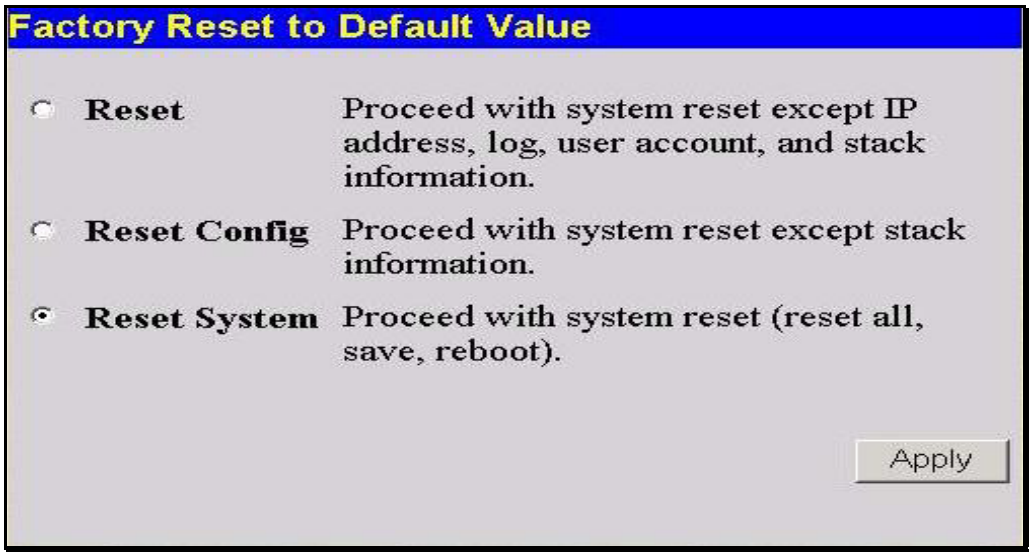


Figure 20-7. Factory Reset

Reboot Device

Clicking the **Yes** click-box will instruct the switch to save the current configuration to non-volatile RAM before restarting the switch.

Clicking the **No** click-box instructs the switch not to save the current configuration before restarting the switch. All of the configuration information entered from the last time **Save Changes** was executed, will be lost.

Click the **Restart** button to restart the switch.

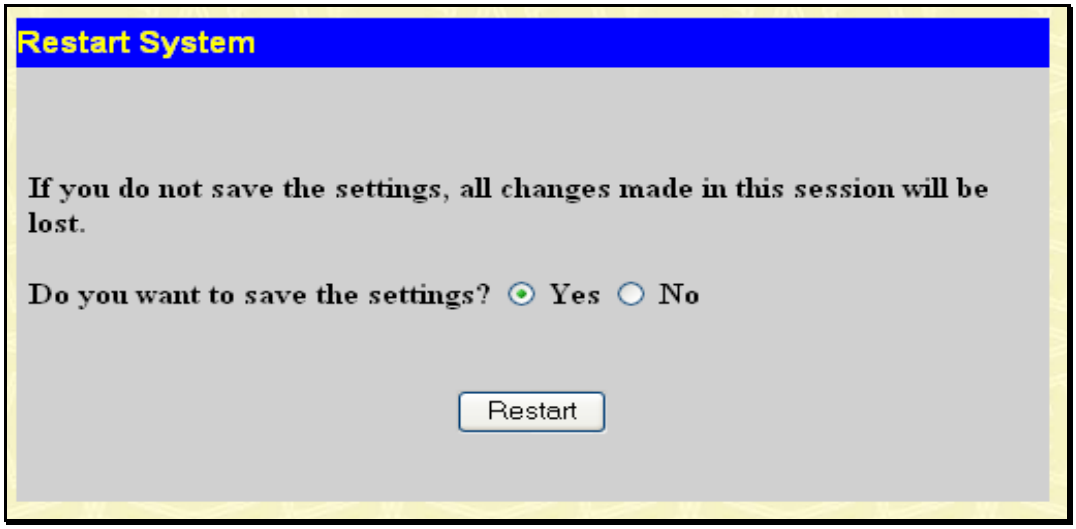


Figure 20-8. Reboot Device

Logout

Use the **Logout** page to logout of the switch's Web-based management agent by clicking on the **Log Out** button.

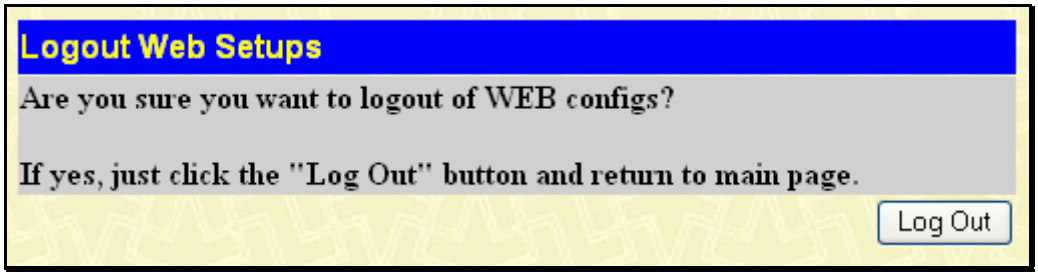


Figure 20-9. Logout

Appendix A

Technical Specifications

General	
Standard	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation
Protocols	CSMA/CD
Data Transfer Rates: **Ethernet** **Fast Ethernet** **Gigabit Ethernet** **Fiber Optic**	Half-duplex Full-duplex 10 Mbps 20Mbps 100Mbps 200Mbps 1000Mbps 2000Mbps IEC 793-2:1992 Type A1a - 50/125um multimode Type A1b - 62.5/125um multimode Both types use SC optical connector
Topology	Ring or Chain
Network Cables	UTP Cat.5 for 100Mbps UTP Cat.3, 4, 5 for 10Mbps EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Physical & Environmental	
AC inputs & External Redundant Power Supply	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	90 watts maximum
DC fans:	2 built-in 40 x 40 x10 mm fans ; 1 built-in 60 x 60 x18 mm fan
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width
Weight:	3.15 kg
EMI:	FCC Part 15 / IECES-003 (Canada) EN55022 / EN50082-1 or EN55024 CE Class A
Safety:	CSA International

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	2 MB per device
Filtering Address Table:	16 K MAC address per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,000 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10 - 1000000 seconds. Default = 300.

Glossary

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

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.

edge port

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. Subset of SNMP MIB II which 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.

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. Herrmann, Fountain Valley, CA 92708-4160, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
INFO: 1-800-326-1688 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.

WARRANTY AND REGISTRATION INFORMATION FOR 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, and 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.

5-Year Limited Warranty for the Product(s) is defined as follows:

- Hardware (excluding power supplies and fans) Five (5) Years
- 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 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: Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office.

- The customer must submit 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 shipping charges to D-Link. No Charge on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products should 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 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.

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.