D-Link ™ DGS-3212SR
12-Port Gigabit Layer 2 Stackable Switch

Manual

TABLE OF CONTENTS

About This Manual

This manual is divided into two general sections:

Basics - Provides a general introduction to the Switch, its hardware and management features, as well as a guide to setting up the Switch hardware and initial configuration.

Web Manager – Describes management and configuration of Switch features, following the layout of the Switch's Web Manager. Each of the Switch's six main folders—Configuration, Security, Management, Monitoring, Maintenance, and Single IP Management—has a separate chapter devoted to it.

Intended Readers

The DGS-3212SR Manual contains information useful for setup and management and of the DGS-3212SR Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [**copy** *filename*] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: **You have mail**. Bold font is also used to represent filenames, program names and commands. For example: use the **copy** command.
`Boldface Typewriter Font`	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Italics	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type *filename* means that you should type the actual filename instead of the word shown in italic.
Menu Name > Menu Option	**Menu Name > Menu Option** - Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices, and Cautions

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

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

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

Safety Instructions

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

⚠ **Safety Cautions**

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

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

- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.

- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.

- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.

- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).

- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.

- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

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

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

  – Unplug the power cable before removing the power supply.

  – If the system has multiple sources of power, disconnect power from the system by

  unplugging *all* power cables from the power supplies.

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

⚠ General Precautions for Rack-Mountable Products

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

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

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

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

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.

Always load the rack from the bottom up, and load the heaviest item in the rack first.

Make sure that the rack is level and stable before extending a component from the rack.

Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.

Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.

Ensure that proper airflow is provided to components in the rack.

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

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

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

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

Protecting Against Electrostatic Discharge

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

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

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

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

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

<div align="right">

Chapter 1

</div>

Introduction

Switch Description

The DGS-3212SR 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 up to twelve DES-3226S Switches in a star 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

- Four built-in combination 10/100/1000BASE-T/SFP ports
- Two additional 4-port modules can be added to stack up to eight additional Switches (IEEE 1394) or up to eight additional Gigabit Ethernet ports (1000BASE-T or SFP) or use combination of stacking and Gigabit Ethernet ports.
- Star topology Switch stacking configuration for up to 12 additional DES-3226S Switches.
- 24 Gbps Switching fabric capacity
- Supports 802.1D STP and 802.1w Rapid Spanning Tree for redundant back up bridge paths
- Supports 802.1Q VLAN
- Supports IGMP snooping
- Supports 802.1p Priority Queues
- Supports 802.3ad LACP Link Aggregation
- Supports port mirroring
- Access Control Profile (ACL)
- Multi-layer Access Control (based on MAC address, IP address, VLAN, Protocol, 802.1p, DSCP)
- Quality of Service (QoS) customized control
- Port Security (MAC address table lock)
- 802.1x (port-based and MAC-based) access control and RADIUS Client support
- Administrator-definable port security
- Per-port bandwidth control
- Broadcast, Multicast and DLF storm 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
- Supports optional external Redundant Power Supply
- Supports Web-based management.
- Supports CLI management.
- Supports BOOTP/DHCP/DNS Relay

- Supports TFTP upgrade
- Supports System Log
- Fully configurable either in-band or out-of-band control via RS-232 console serial connection.
- Telnet remote control console
- Simple Network Time Protocol
- MAC address update notification
- Web GUI Traffic Monitoring
- Supports Single IP Management v.1.0
- Supports Traffic Segmentation

Front Panel Components

The front panel of the Switch consists of LED indicators, an RS-232 communication port, two slide-in module slots, and four 1000BASE-T/SFP combo ports.
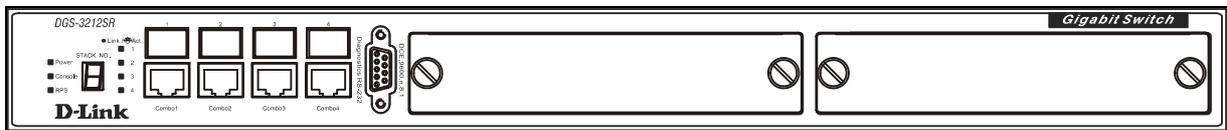
Figure 1-1. Front Panel View of the Switch as shipped (no modules are installed)

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.

A front-panel slide-in module slot for Gigabit Ethernet ports can accommodate a 4-port 1000BASE-T Gigabit Ethernet module, a 4-port Gigabit Ethernet SFP module, or a stacking module to connect to four DES-3226S Switches.

LED Indicators

The LED indicators of the Switch include Power, Console, and Link/Act. The following shows the LED indicators for the Switch along with an explanation of each indicator.
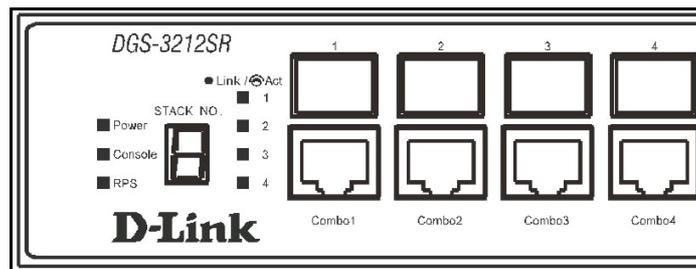
Figure 1-2. LED Indicators

Power	This indicator on the front panel should be lit during the Power-On Self Test (POST). It will light green approximately two seconds after the Switch is powered on to indicate the ready state of the device.
Console	This indicator is lit 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.

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.

See below for description of Stack ID LED indicator.

NOTICE: The **Stack ID** LED on the Switch's front panel will display an **F**, regardless of the Switch's stacking mode (Master Switch in a Switch stack, or Standalone mode).

Stacking LED Indicators

Stacking LED indicators include the Stack ID indicator on the front panel and the Link/Act indicators on the front of the DEM-540 stacking module.

NOTICE: The four build-in combination ports on the front panel of the DGS-3212SR can be configured as stacking ports using the CLI.

Each stacking module has a single **Link/Act** LED indicator on its front panel for each IEEE 1394 IN/OUT pair.
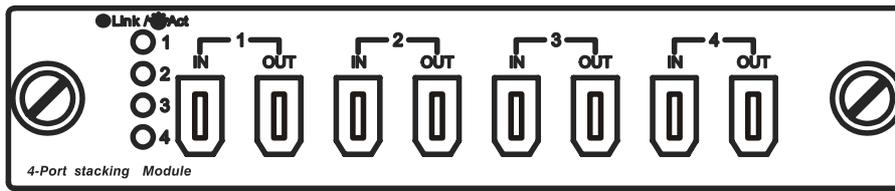
Figure 1-3. Front panel of DEM-540 IEEE 1394 stacking module

Link/Act	The Link/Act LEDs have the same function as the corresponding LEDs for the Switch's built-in Gigabit Ethernet ports. The Link LED lights to confirm a valid link, while the Act LED blinks to indicate activity on the link.
Stack ID	The Switch includes a digital indicator to indicate the Switch status in a stacked Switch group. An "F" indicates the Switch is acting in the capacity of a master Switch of a stacked group of DGS-3212SR/DES-3226S Switches. The remaining slave Switches in the group will display a corresponding stack number (1-C) to indicate the logical position of the slave Switch in the stacked group. See the discussion of Switch Stacking below for more information on stacking DGS-3212SR/DES-3226S Switches.

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

Rear Panel Description

The rear panel of the Switch contains an AC power connector.

Figure 1-4. Rear panel view of the Switch

The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 ~ 240 VAC at 50 ~ 60 Hz.

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-200 or RPS-500 redundant power supply units.

Plug-in Modules

The DGS-3212SR Switch is able to accommodate optional plug-in modules in order to increase functionality and performance. Two modules may be installed and used in combination with any of the three available modules. Plug-in modules must be purchased separately.

## DEM-340T 1000BASE-T Module
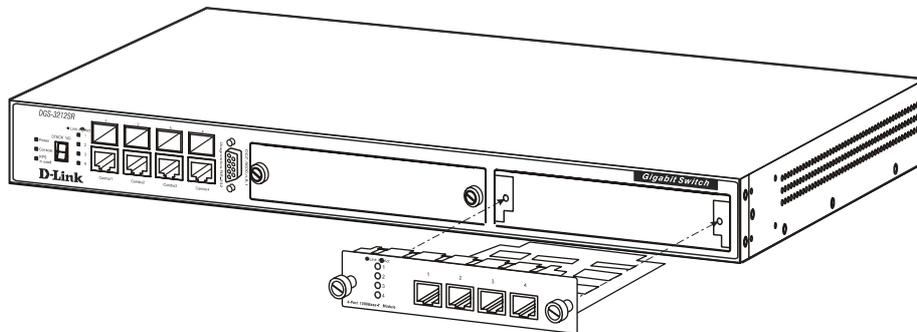
Figure 1-5. 1000BASE-T Four-port module

- Front-panel module
- Connects to 1000BASE-T devices
- LED indicators for Link/Activity

## DEM-340MG SFP (Mini GBIC) Module
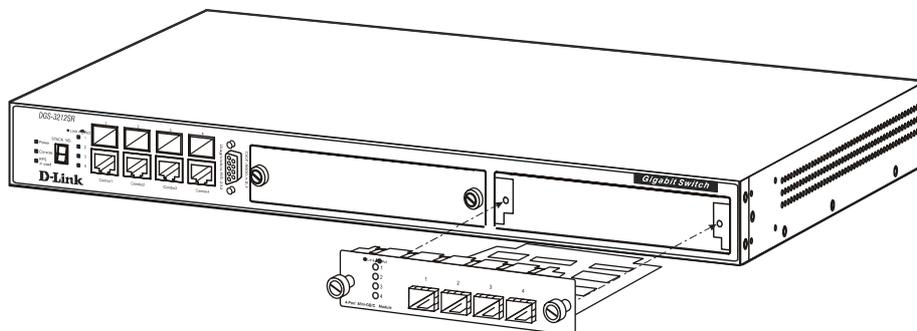
Figure 1-6. Four-port Gigabit SFP module

- Front-panel module
- Connects to Gigabit Ethernet devices
- LED indicators for Link/Activity and Status

4

DEM-540 IEEE 1394 Stacking Module
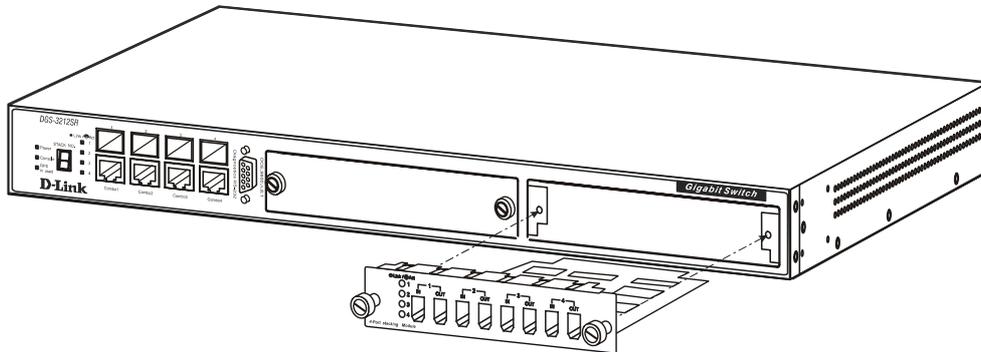
Figure 1-7. DEM-540 IEEE 1394 Stacking module

- Front-panel module

- Connect to four DES-3226S Switches (up to eight additional slave units may be stacked)

- Four transmitting ports and Four receiving port

- Use the connector of IEEE 1394b

- Data rate up to 1000 Mbps

- 8-segment LED display to indicate Switch ID number within the Switch stack

Switch Stacking

The DGS-3212SR can be stacked with a DES-3226S, functioning as a Master of the stack. There are two connection options available to for stacking. One option is to use the built-in combination ports (1000BASE-T/SFP). The other possibility is to install one or two DEM-540 stacking modules and complete the stacking connection through the IEEE 1394 stacking ports. With two stacking modules installed, the DGS-3212SR can be stacked with as many as twelve slave units.

Each optional stacking module allows up to four DES-3226S Switches to be interconnected in a stack with the DGS-3212SR. Two stacking modules may be used to form a nine-Switch stack consisting of one Master and eight Slaves, managed through the DGS-3212SR Master Switch. The stacked group has a single IP address and is managed as a single device. The entire Switch stack is managed and monitored through the network or alternatively, through the serial port on the DGS-3212SR. The stacking modules connect to the slaves using IEEE 1394 serial cable (Firewire) in a star topology for DES-3226S groups (see illustration on page 8).

The stacking ports are marked **IN** and **OUT**. The IEEE 1394 compliant cable must be connected from an **IN** port on one Switch to an **OUT** port on the next Switch in the stack.

Restrictions and Cautions for Stacking

The DGS-3212SR may serve as the Master of up to twelve additional Switches. The slave Switch units must meet the following criteria:

- All additional slave Switches must be the same model, that is (at the time of the writing of this manual), the slaves must be all DES-3226S Switches. The slave unit types cannot be mixed within a single stacked group.

- DES-3226S slave Switches must have firmware Release IV or later loaded to operate properly with the DGS-3212SR Master.

- The DGS-3212SR is automatically started as the Master Switch in a Switch stack.

- It is necessary to enable stacking for each slave Switch in a stacked group before interconnecting them and before connecting the group to the network. Stacking can be enabled by connecting to each slave through the console port and using the CLI stacking configuration command. Before stacking has been

enabled on the slaves, the IEEE 1394 port is treated logically as an individual 1000BASE port in full-duplex mode. Since the Spanning Tree Protocol is disabled by default, a broadcast storm will result if the stacking link is completed between Switches that have not been properly configured.

NOTICE: The CLI stacking command set for the DGS-3212SR is slightly different from the CLI stacking command set for the DES-3226S. Please refer to the CLI Reference Manual for each Switch for details or read the instructions starting on page 12 below.

Management Options

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

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 Opera, 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 Manual, 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:

- RFC 1643 Ether-like MIB
- RFC 1724 RIPv2 MIB
- RFC 1757 RMON
- RFC 1850 OSPF MIB
- RFC 1907 SNMPv2 MIB
- RFC 2021 RMON II MIB
- RFC 2096 IP-FORWARD MIB
- RFC 2233 IF-MIB
- RFC 2358 Ethernet-Link MIB
- RFC 2573 SNMP Notification and Target MIB
- RFC 2574 SNMP User-based SM MIB
- RFC 2575 SNMP View-based ACM MIB
- RFC 2674 802.1p and 802.1q Bridge MIB
- RFC 2737 Entity MIB
- RFC 2932 IPMROUTE STD MIB

- RFC 2933 IGMP MIB
- RFC 2934 PIM MIB
- IEEE8021-PAE 802.1x PAE MIB
- D-Link Enterprise MIB

Chapter 2

Installation

Package Contents
Before You Connect to the Network
Installing the Switch without a Rack
Installing the Switch in a Rack
Connecting Stacked Switch Groups
Configuring a Switch Group for Stacking
External Redundant Power System
Connecting the Console Port
Password Protection
SNMP Settings
IP Address Assignment
Connecting Devices to the Switch

Package Contents

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

- One DGS-3212SR Layer 2 Switch

- Mounting kit: 2 mounting brackets and screws

- Four rubber feet with adhesive backing

- One AC power cord

- This Manual

- CLI Reference

Before You Connect to the Network

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.

> **NOTICE**: Do not connect the Switch to the network until you have established the correct IP settings, user accounts and proper stacking configuration (if the Switch is stacked).

Installing the Switch without the Rack

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.

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.
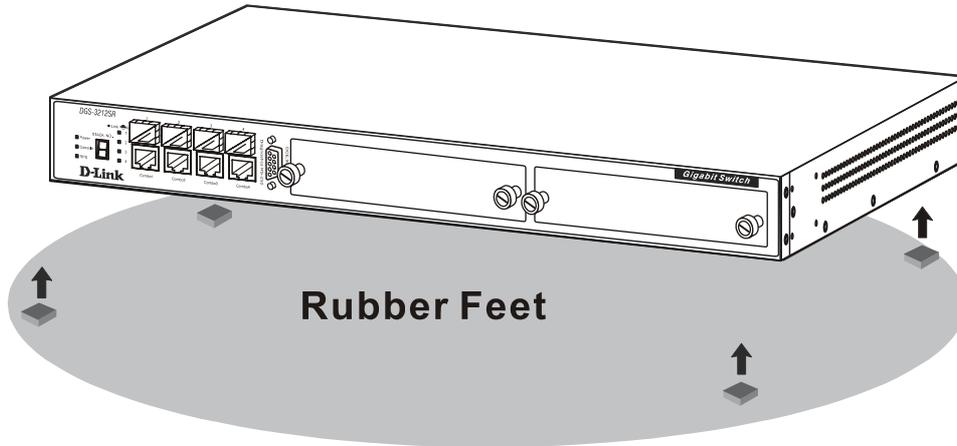

Figure 2-1. Install rubber feet for installations with or without a rack

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.
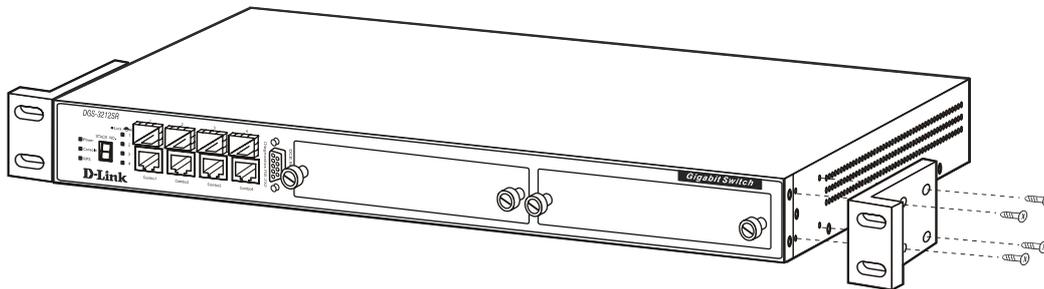
**Figure 2-2. Attach mounting brackets**
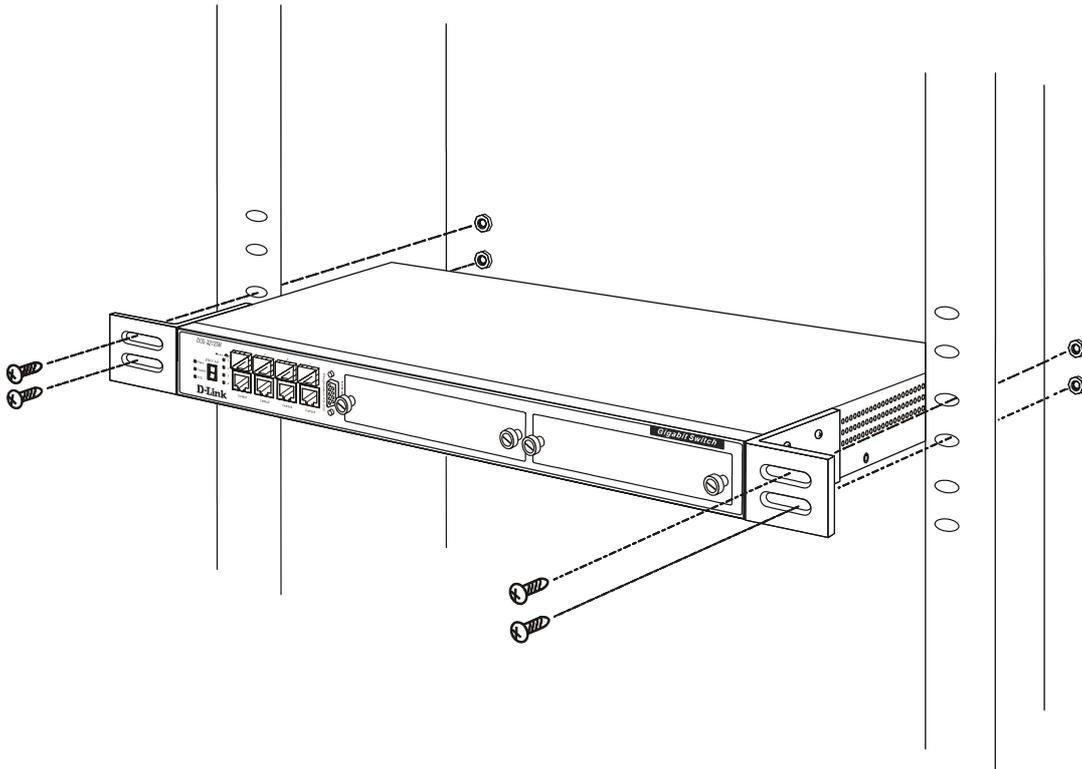
Figure 2-3. Install Switch in equipment rack

Connecting Stacked Switch Groups

The DGS-3212SR may be configured to function as the Master of a stacked group of DES-3226S Switches (see Restrictions for Stacking on page 5). A stacked group of DES-3226S Switches are connected using a star topology. The instructions below, Configuring a Switch Group for Stacking, tell you how to configure the DGS-3212SR to function as a Master, as well as how to configure the DES-3226S to function as a slave Switch units using the CLI interface.

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

Stacking Connections with IEEE 1394 Cabling and Ethernet

DGS-3212SR
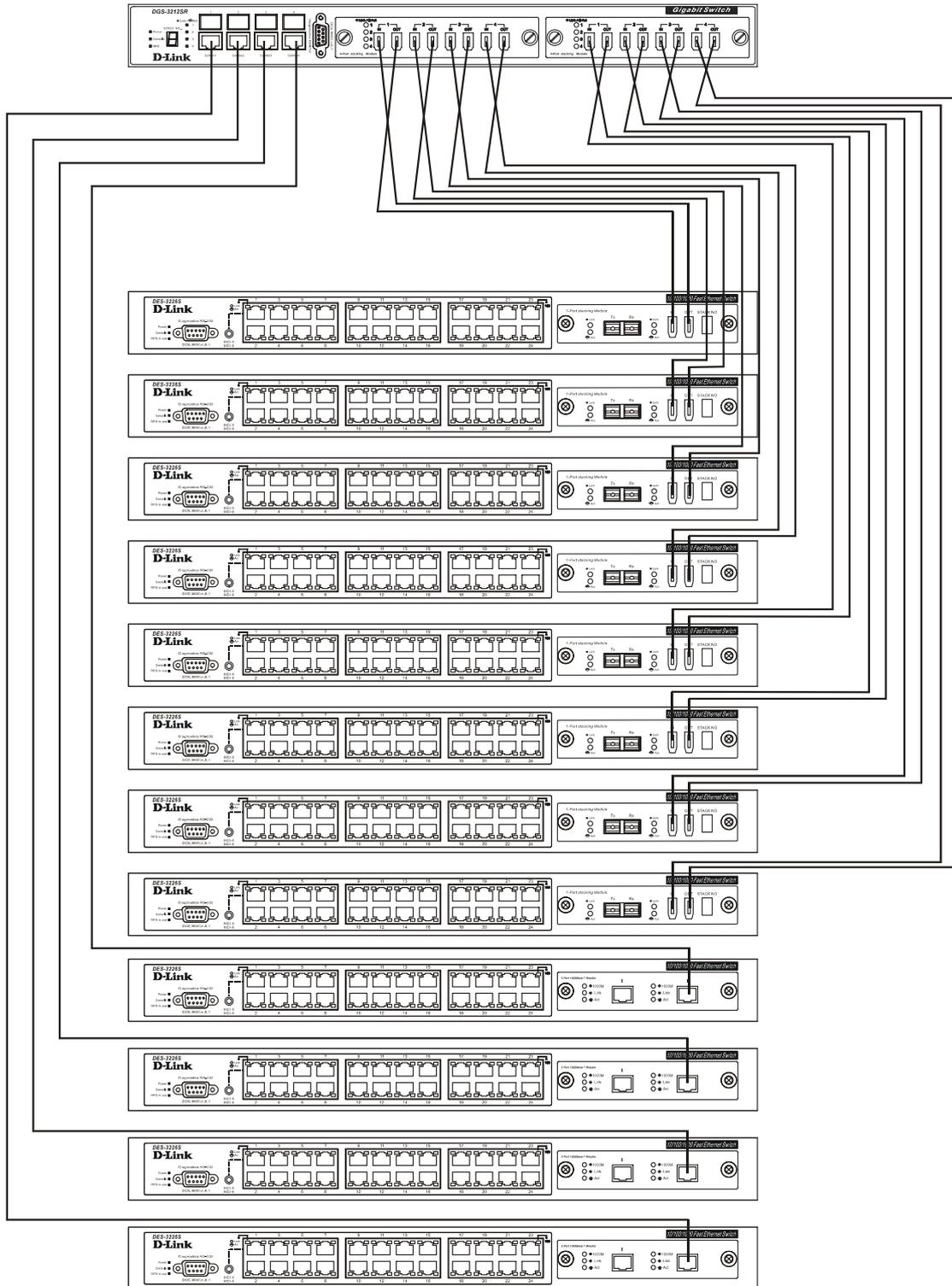
Figure 2-4. Star Topology Stacked Switch Group

The stacking ports are marked **IN** and **OUT**. The IEEE 1394 compliant cable must be connected from an **IN** port on one Switch to an **OUT** port on the next Switch in the stack.

Configuring a Switch Group for Stacking

Follow the instructions below to first configure the slave units, and then to configure the DGS-3212SR as the designated Master.

NOTICE: The DGS-3212SR can be used to manage a Switch stack consisting of only DES-3226S Switches.

For the DES-3226S the stacking configuration as a Master or Slave Switch is no longer necessary. The DGS-3212SR can communicate with a DES-3226S regardless of its stacking configuration. It is recommended that you configure all DES-3226S Switches in a Switch stack in the auto stacking mode to reduce the potential for problems. The default stacking mode configuration for the DES-3226S is auto.

To configure the DES-3226S to function in a stacked group as a slave, do the following:

1. At the CLI login prompt, enter `config stacking mode enable auto` and press the **Enter** key.

2. You will be prompted to save the stacking mode configuration. Press the Y key (yes) to save the stacking mode configuration.

3. Successful configuration will be verified by a **Success** message. It takes a few seconds for the change to take effect and be saved. See the example below for the DES-3226S.

```
DES-3226S:4#config stacking mode enable auto
Command: config stacking mode enable auto


Do you want to save the new system configuration to NV-RAM now?(y/n)
Saving all configurations to NV-RAM... Done.
Success.


DES-3226S:4#............
```

The default settings for the DGS-3212SR has the stacking mode enabled. However if the stacking mode has been disabled it will be necessary to enable it. Follow the instructions below to change the stacking mode to enable. If you do not know what the stacking mode setting currently is, use the command `show stacking mode`.

To enable stacking in the DGS-3212SR, do the following:

1. At the CLI login prompt, enter `config stacking mode enable` and press the **Enter** key.

2. You will be prompted to save the stacking mode configuration. If you save the new stacking mode by pressing the Y key, the settings will be saved and the Switch will restart.

3. Press the Y key (yes) to save the stacking mode configuration and restart the Switch.

```
DGS-3212SR:4#config stacking mode enable
Command: config stacking mode enable
```

> **The new stacking mode configuration must be saved and the system restarted**
>
> **to put the new settings into effect.**
>
> **If you do not save the changes now, they will be lost.**
>
> **Saving all configurations to NV-RAM... 15%**

Changing the stacking mode in the DGS-3212SR will automatically save the settings and restart the system. It will take a few minutes to complete the process.

Unit ID Display for Switches in a Switch Stack

The Stack ID 7-segment LED (as shown below) on the front panel of the DGS-3212SR will always display F (15 in hex). An F will also be displayed in the Stack ID LED even if the DGS-3212SR is in standalone mode.
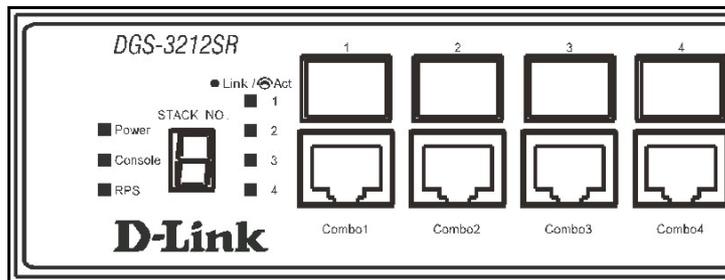

Figure 2-5. DGS-3212SR Front Panel

The Unit ID of individual DES-3226S Switches in a Switch stack is determined by the port number of the port on the DGS-3212SR that the Switch is connected to. The ports on the DGS-3212SR are numbered starting with port 1 from left to right along the front panel of the Switch. For example, the four combination ports next to the Stack NO. LED are numbered 1 through 4, so if a four port stacking module is installed in the first module slot, the stacking ports will be numbered 5 through 8. If two stacking modules are installed in the DGS-3212SR, then the stacking ports on the second module will be numbered 9 through 12.
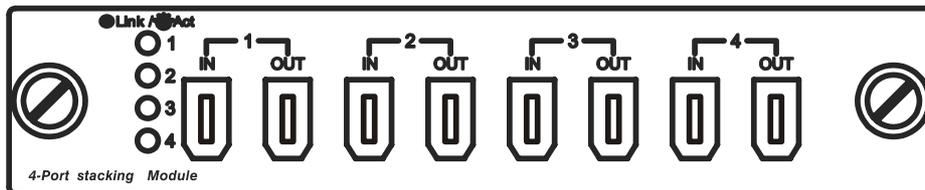

Figure 2-6. DEM-540 Stacking Module Front Panel

If the a stacking module is installed in the DGS-3212SR's first module slot, then the first IN/OUT pair in the figure above will be port 5. If a DES-3226S in a Switch stack is connected to the first stacking port (port number 5 on the DGS-3212SR), then the Unit ID of the DES-3226S will be 5.

The Unit ID of the DES-3226S will be displayed in the STACK NO. LED on the front panel of the DES-3226S's stacking module, as shown below.
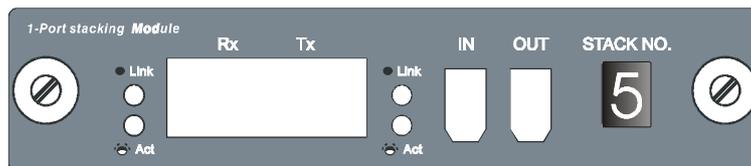

Figure 2-7. DES-3226S Stacking Module Front Panel

External Redundant Power System

The Switch supports an external redundant power system.
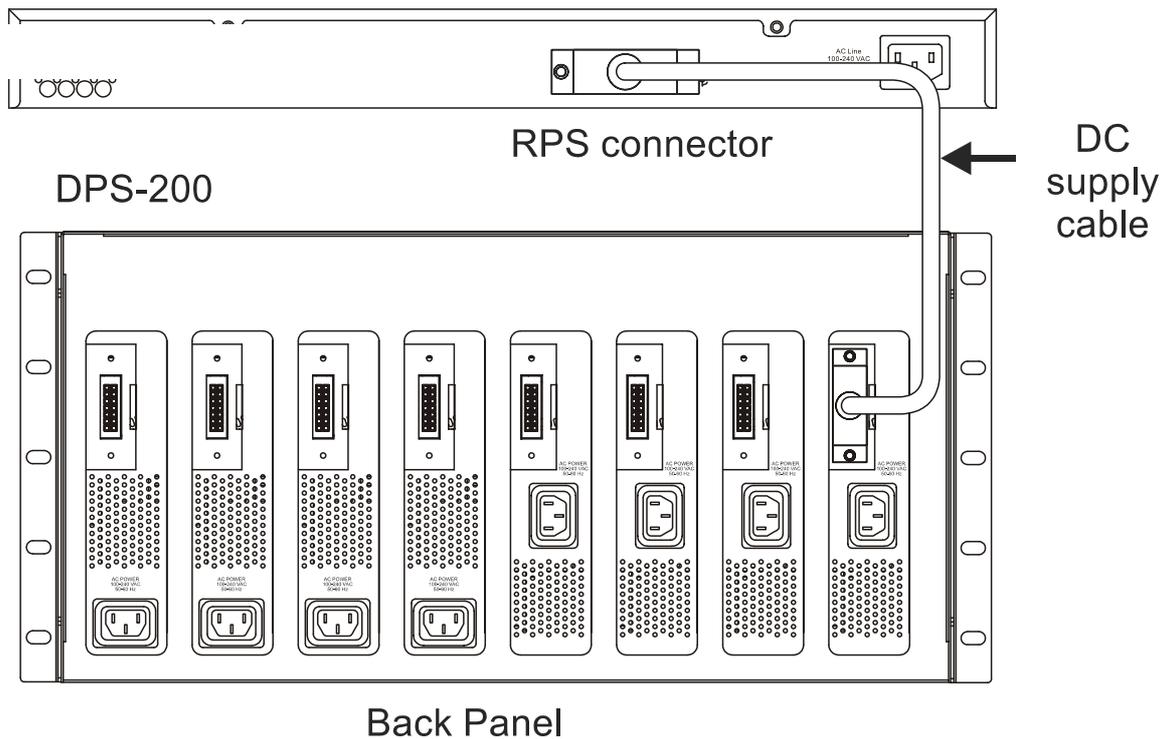
Figure 2-8. DPS-200 with DGS-3212SR

NOTE: See the DPS-200 documentation for more information.

CAUTION: Do not use the Switch with any redundant power system other than the DPS-200 or 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 male DB-9 connector, implemented as a data terminal equipment (DTE) connection.

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

- A terminal or a computer with both a serial port and the ability to emulate a terminal

- A null modem or crossover RS-232 cable with a female DB-9 connector for the console port on the Switch

To connect a terminal to the console port:

1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.

2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:

   a. Select the appropriate serial port (COM port 1 or COM port 2).

   b. Set the data rate to 9600 baud.

   c. Set the data format to 8 data bits, 1 stop bit, and no parity.

   d. Set flow control to `none`.

   e. Under **Properties**, select **VT100 for Emulation** mode.

   f. 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.

   g. 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.

   h. After the boot sequence completes, the console login screen displays.

   i. 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.

   j. 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.

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

Password Protection

The DGS-3212SR 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-3212SR: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) 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-3212SR 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.

```
Boot Procedure                                                    2.00.001
-----------------------------------------------------------------------------
Power On Self Test .................................... 100 %

MAC Address   : 00-80-C8-32-12-E0
H/W Version   :

Please wait, loading Runtime image ..................... 100 %
```

Figure 2-9. 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 that can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

```
            DGS-3212SR Gigabit Ethernet Switch Command Line Interface

                            Firmware: Build 2.00-B09
                Copyright(C) 2000-2003 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DGS-3212SR:4#config ipif System ipaddress 10.22.24.9/255.0.0.0
Command: config ipif System ipaddress 10.22.24.9/8

Success.

DGS-3212SR:4#
```

Figure 2-10. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.22.24.9 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.

<div style="border:1px solid black; display:inline-block; padding:8px;">

Chapter 3

</div>

Basic Switch Management

Before You Start
Web-based User Interface
Basic Setup
Switch Information
Switch IP Settings
Security IP Management Stations
User Accounts Management
Saving Changes
Factory Reset
Restart System
Advanced Settings
Switch Stack Management

All software function of the DGS-3212SR can 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 Opera, 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.

Before You Start

The DGS-3212SR Layer 2 Switch supports a wide array of functions and gives great flexibility and increased network performance.

This flexibility and rich feature set requires a bit of thought to arrive at a deployment strategy that will maximize the potential of the DGS-3212SR Layer 2 Switch. Please read the portions of this manual pertaining to the functions you wish to perform with the Switch.

Web-based User Interface

The user interface provides access to various Switch configuration and management windows, 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 three distinct areas as described in the table below.
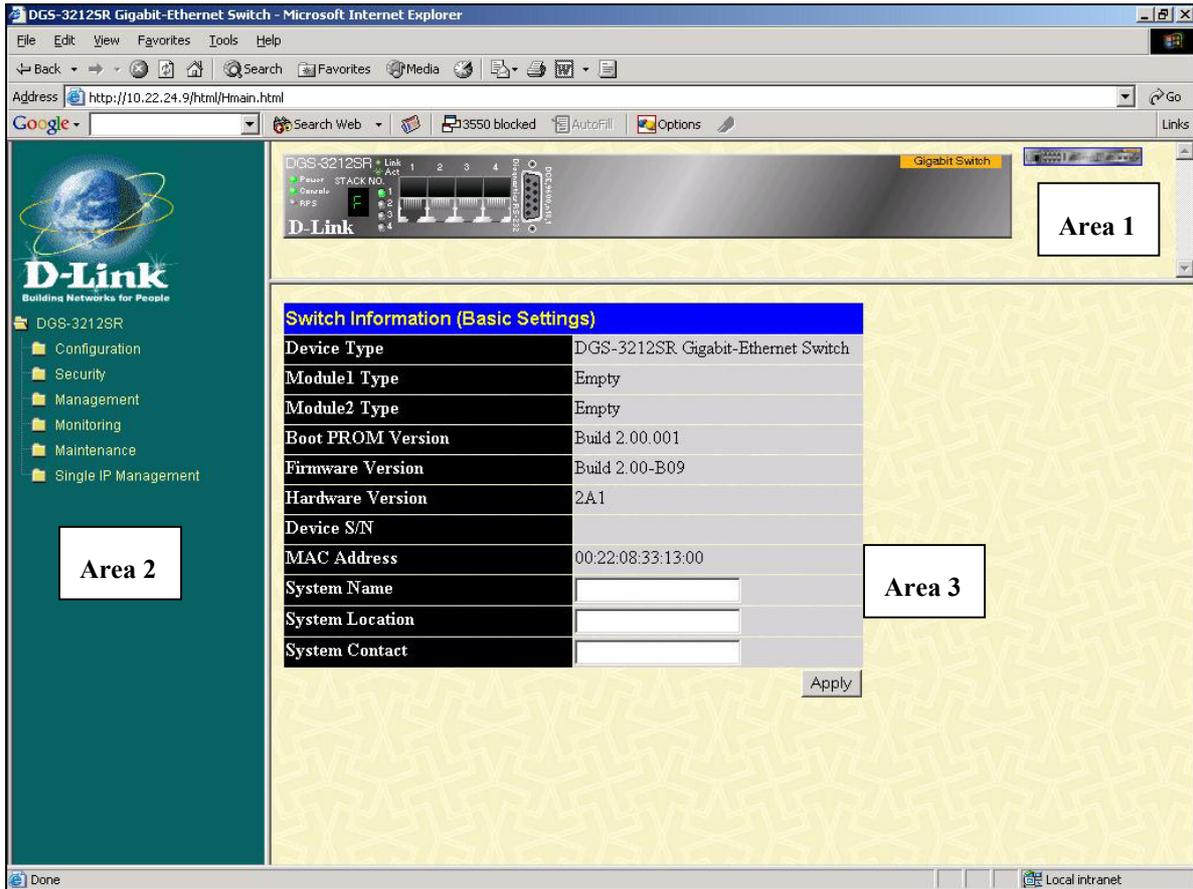
Figure 3-1. Main Web-Manager window

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. When the Switch is stacked a virtual representation of the Switch stack appears in the right hand portion. Click on the ports in the front panel to manage the port's configuration or view data for the port.
2	Select the window to be displayed. The folder icons can be opened to display the hyperlinked window buttons and sub-folders contained within them.
3	Presents the information selected for configuration or display.

Login to Web Manager

To begin managing the 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 Welcome page, click on the Login hyperlink; this opens a login dialog box. Enter a user name and password to access the Switch's management main page (pictured above). There is no user name or password configured for the Switch in the default settings, so if this is the first time logging in it is not necessary to enter these.

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

Web Pages and Folders

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

Configuration: This folder includes all the sub-folders and windows used to configure various performance functions of the Switch.

Security: This folder contains the Port Access Entity (PAE) sub-folder used to configure 802.1x and RADIUS server settings. The Trusted Host window link is located here as well.

Management: The windows used to configure SNMP settings, management IP stations, and user accounts are located here.

Monitoring: Data tables for performance statistics, application and protocol status are contained in the links and subfolders of this folder.

Maintenance: Contains windows 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.

Single IP Management: SIM settings, Topology, Firmware Update, and Configuration Backup/Restore windows are located here.

NOTE: Be sure to configure the user name and password in the User Accounts window 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

The first page displayed upon logging in is the **System Information (Basic Settings)** window. This window can be accessed at any time by clicking the **Switch Information** button in the **Configuration** folder.

Figure 3-2. Switch Information (Basic Settings) window

This window displays general information about the Switch including its MAC Address, Hardware Boot PROM and Firmware versions, and installed module information.

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 **Switch IP Settings** window located in the **Configuration** folder.

To configure the Switch's IP address:

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

Figure 3-3. Switch IP Settings window

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

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

- Select *Manual* from the Get IP From drop-down menu.

- Enter the appropriate IP address and subnet mask.

If you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the gateway. If you will manage the Switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.

If no VLANs have been previously configured on the Switch, you can use the default VLAN 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 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 Management Station IP Addresses (see page 24) are assigned or SNMP settings are configured to control management.

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 that 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

Use the **Security IP Management** window to define up to four community strings. Community strings are used to verify who can receive SNMP information from the Switch.

To access the **Security IP Management** window, click **Trusted Host** in the **Security** folder.

Figure 3-4. Security IP Management window

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 in the area provided and then click the **Apply** button.

User Account Management

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

Figure 3-5. User Account Management window

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- 6. User Account Modify Table window

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.

25

Figure 3- 7. User Account Modify Table window

Modify or delete an existing user account in the **User Account Modify Table** window. 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.

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

Table 3- 1. Admin and User Privileges

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

Save Changes

Changes made to the Switch's configuration must be saved in order to retain them. Access the **Save Configuration** window by clicking the **Save Changes** button located in the **Maintenance** folder.
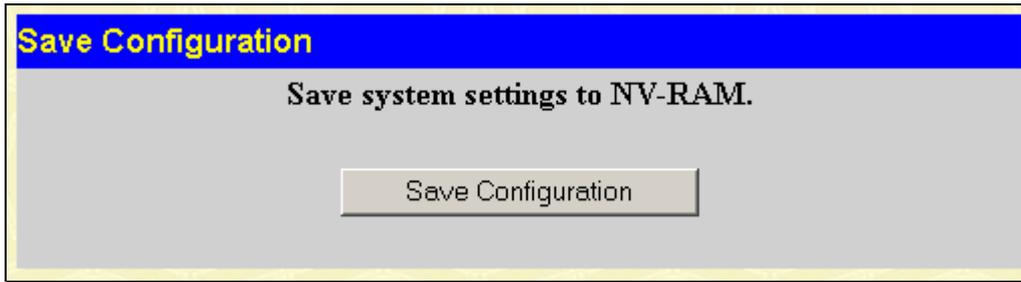
Figure 3- 8. Save Configuration window

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.

Factory Reset

Click the **Factory Reset** link in the **Maintenance** folder to bring up the following window.
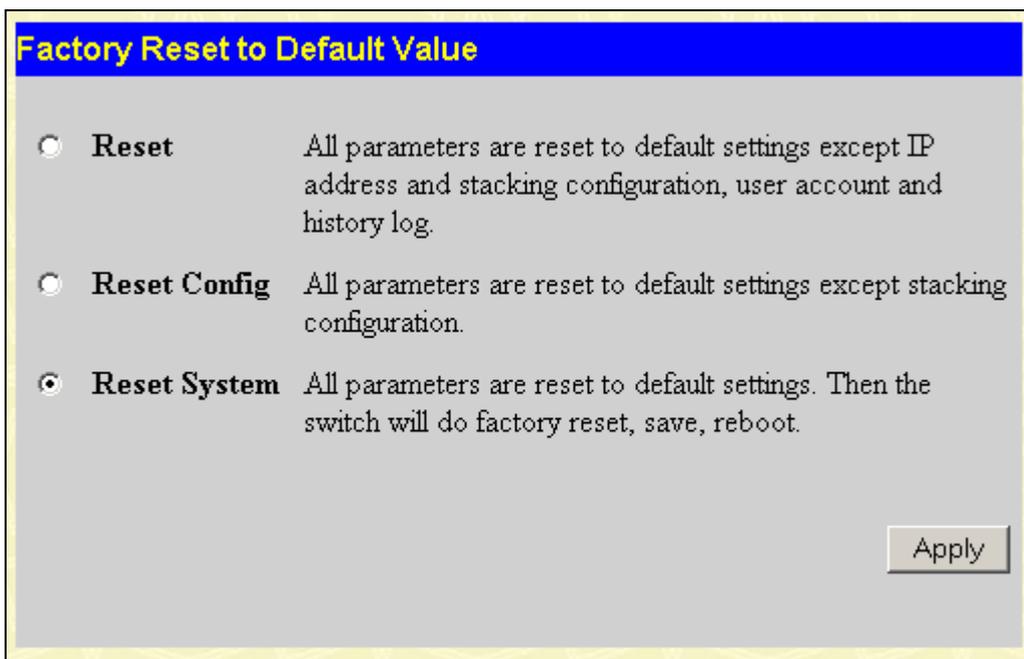
Figure 3- 9. Factory Reset to Default Value window

The following options are available to perform a factory reset:

- **Reset** – Returns all configuration settings to the factory default settings except the Switch's stacking mode, IP address, subnet mask, and default gateway settings.

- **Reset Config –** Returns all configuration settings to the factory default settings except the stacking mode configuration, 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.

27

- **Reset System –** Returns all configuration 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 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.

Select the reset option you want to perform and click on the **Apply** button.

Restart System

The following window is used to restart the Switch. Access this window by clicking on the **Restart System** 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 from the last time **Save Changes** was executed will be lost.

Click the **Restart** button to restart the Switch.
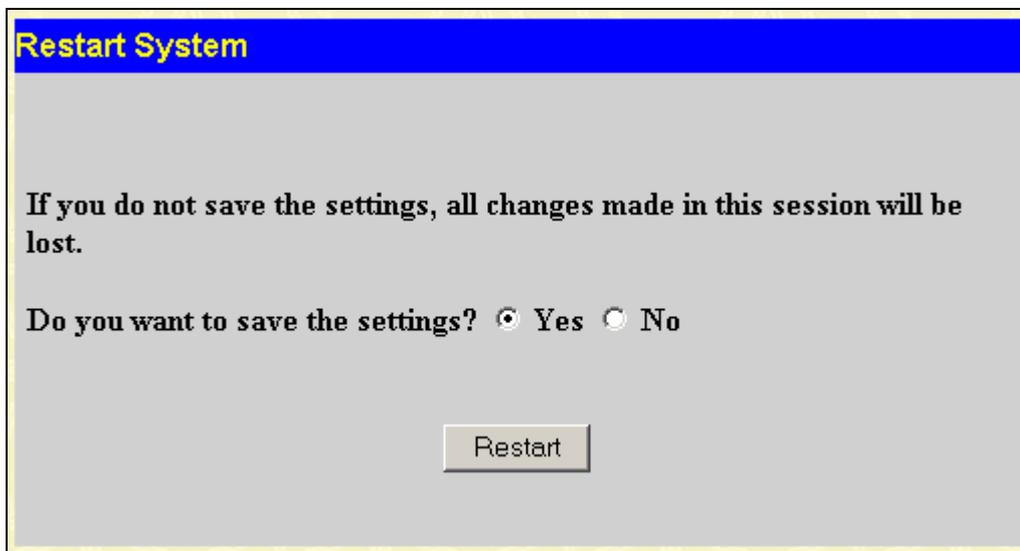
Figure 3- 10. Restart System window

NOTE: Clicking Yes is equivalent to executing Save Changes and then restarting the Switch.

Advanced Settings

Figure 3- 11. Switch Information (Advanced Settings) window

The Advanced Settings options are summarized in the table below:

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	Select the baud rate used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: *9600, 19200, 38400* or *115200*.
MAC Address Aging Time (10-1000000)	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** window in 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,

Only	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*.
Telnet TCP Port Number(1-65535)	The Telnet TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Telnet protocol is 23.
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.
Web TCP Port Number(1-65535)	The TCP port number currently being utilized by the Switch to connect to the web interface. The "well-known" TCP port for the Web interface is 80.
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 *MAC Source, MAC Destination*, *MAC Src & Dest, IP Source, IP Destination*, and *IP Src & Dest.* (See Link Aggregation)
Switch 802.1x	Use this pull-down menu to enable or disable 802.1x functions on the Switch.
Syslog state	Use this pull-down menu to enable or disable Syslog.

Switch Stack Management

The DGS-3212SR Switch can be used as a standalone high-capacity Switch or be used in a stacked arrangement. There are two hardware requirements to use the Switch in a stacked group:

1. The proper module(s) must be installed. One or two DEM-540 Stacking modules must be installed in order to use the Switch in a stacked configuration.

2. Slave Switch units in a stacked Switch group must be uniform in type and model, furthermore they must be one of the Switch models intended for use with the DGS-3212SR, namely DES-3226S Switches.

One stacking module can be installed to stack up to four additional slave Switch units or two modules can be installed to stack up to eight additional slave Switch units.

Configure Stacking

The web manager can be used to enable or disable the stacking mode and to enable stacking for any of the built-in combination ports.

The Switch stack displayed in the upper right-hand corner of your web-browser is a virtual representation of the actual stack (see example below). The icons appear in the same order as their respective Switches.

When the Switches are properly interconnected, information about the resulting Switch stack is displayed in the **Stack Mode Setup** window. To view stacking information or to enable/disable the stacking mode, click the **Stack Information** link in the **Monitoring** folder.

Figure 3- 12. Stack Mode Setup (stacking disabled) window

To enable the stacking mode, follow the steps listed below.

1. Select *Enabled* from the Stack Mode State drop-down menu.

2. Click on the **Apply** button.

To enable stacking for one or more built-in combination ports, do the following:

1. Select *Enabled* from the Stack Mode State drop-down menu.

2. Select the Stack Port by clicking to check a corresponding selection box.

The Stack Information Table displays the read-only information listed in the table on the next page.

The current order in the Switch stack is also displayed on the front panel of each slave Switch, under the STACK NO. heading. The Stack ID LED display on the front panel of the DGS-3212SR will always display an F (15 in hex), regardless of whether the DGS-3212SR is the master Switch in a Switch stack or in standalone mode.

Below is an example of the **Stack Mode Setup** window with stacking mode enabled on Ports 9-12.

31

Stack Mode Setup

Stack Topology	Auto Detect
Setting	MASTER
Current	MASTER
Stack Mode State	Enable
Stack Port	1 2 3 4 5 6 7 8 9 10 11 12 ☑ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☑ ☑ ☑ ☑

Apply

Total Entries : 2

Stack Information Table

ID	MAC Address	Port Range	Mode	Version	RPS Status	Model Name
15	00-47-44-00-32-00	1-12	MASTER	2.00-B09	Present	DGS-3212SR
10	00-01-02-41-44-01	501-526	SLAVE	4.02-B03	Not Support	DES-3226S

Figure 3- 13. Stack Mode Setup (stacking enabled) window

Variables in this window are described below:

Parameter	Description
ID	Displays the Switch's order in the stack. The Switch with a unit id of 1 is the master Switch.
MAC Address	Displays the unique address of the Switch assigned by the factory.
Port Range	Displays the total number of ports on the Switch. Note that the stacking port is included in the total count.
Mode	Displays the method used to determine the stacking order of the Switches in the Switch stack.
Version	Displays the version number of the stacking firmware.
RPS Status	Displays the status of an optional Redundant Power Supply.
Model Name	Displays the model name of the corresponding Switch in a stack.

When the stacked group is connected and properly configured, the virtual stack appears in the upper right-hand corner of the web page.

Figure 3- 14. Stack Information web page

Chapter 4

Configuration

Switch Information
IP Address
Advanced Settings
Port Configuration
Port Mirroring
Link Aggregation
LACP Port Settings
Port Access Entity
802.1X Authenticator Settings
PAE System Control
802.1X Capability Settings
Initialize Port(s)
Reauthenticate Port(s)
Radius Server
IGMP
IGMP Snooping
Static Router Ports Entry
Spanning Tree
STP Switch Settings
STP Port Settings
Forwarding & Filtering
Unicast Forwarding
Multicast Forwarding
Multicast Port Filtering Mode
VLANs
Static VLAN Entry
GVRP Setting
QoS
802.1p Default Priority
802,1p User Priority
QoS Output Scheduling
Traffic Segmentation
Bandwidth Control
MAC Notification
Global Settings
Port Settings
System Log Server
Port Security
SNTP Setting
Time Setting
Time Zone and DST
Access Profile Table

The DGS-3212SR's Web interface is divided into six main folders: **Configuration**, **Security**, **Management**, **Monitoring**, **Maintenance**, and **Single IP Management**. This chapter describes all of the **Configuration** sub-folders and windows.

Switch Information

The first page displayed upon logging in is the **System Information (Basic Settings)** window. This window can be accessed at any time by clicking the **Switch Information** button in the **Configuration** folder.

Figure 4- 1. Switch Information (Basic Settings) window

This window displays general information about the Switch including its MAC Address, Hardware Boot PROM and Firmware versions, and installed module information.

IP Address

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 **Switch IP Settings** window located in the **Configuration** folder.

To configure the Switch's IP address:

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

Figure 4- 2. Switch IP Settings window

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

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

- Select *Manual* from the Get IP From drop-down menu.

- Enter the appropriate IP address and subnet mask.

If you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the gateway. If you will manage the Switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.

If no VLANs have been previously configured on the Switch, you can use the default VLAN 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 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** window. 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 Management Station IP Addresses are assigned or SNMP settings are configured to control management access.

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 that 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.

Advanced Settings

Figure 4- 3. Switch Information (Advanced Settings) window

The Advanced Settings options are summarized in the table below:

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	Select the baud rate used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: *9600, 19200, 38400* or *115200*.
MAC Address Aging Time (10-1000000)	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** window in 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.

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*.
Telnet TCP Port Number(1-65535)	The Telnet TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Telnet protocol is 23.
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.
Web TCP Port Number(1-65535)	The TCP port number currently being utilized by the Switch to connect to the web interface. The "well-known" TCP port for the Web interface is 80.
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 *MAC Source, MAC Destination*, *MAC Src & Dest, IP Source, IP Destination*, and *IP Src & Dest.* (See Link Aggregation)
Switch 802.1x	Use this pull-down menu to enable or disable 802.1x functions on the Switch.
Syslog state	Use this pull-down menu to enable or disable Syslog.

Port Configuration

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

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

Figure 4- 4. Port Configuration window

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 in the table below.

The configurable parameters for ports include the following:

Parameter	Description
State <*Enabled*>	Toggle the State field to either enable or disable a given port.
Speed/Duplex <*Auto*>	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. *Auto* – auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *1000M/Full*, *1000M/Half*, *100M/Full*, *100M/Half, 10M/Full,* and *10M/Half.* 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.

Port Mirroring

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. Follow the steps below to set up port mirroring.

Figure 4- 5. Setup Port Mirroring window

To configure a mirror port:

1. Select the Source Unit containing the port that is being mirrored.

2. Configure how the port is to be mirrored by selecting the direction that will be mirrored. Choose Ingress, Egress, or Both for the mirrored port by clicking the appropriate radio button for the port.

3. Select the Target Port using the Unit and Port drop-down menus.

4. Change the Status drop-down menu to *Enabled*.

5. 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.

Traffic Control

Use the **Traffic Control Setting** window 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.

Figure 4- 6. Traffic Control Setting window

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 stack – 15 for a Switch in standalone mode) 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*.

Link Aggregation

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 six link aggregation groups, each group consisting of up of up to eight links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the two (optional) Gigabit ports – which can only belong to a single link aggregation group. A link aggregation group may not cross an 8-port boundary, starting with port 1 (a group may not contain ports 8 and 9, for example) and

all of the ports in the group must be members of the same VLAN. Further, the aggregated links must all be of the same speed and should be configured as full duplex.

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

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

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

To configure port trunking, click on the **LACP** hyperlink in the **Configuration** folder and then click **Link Aggregation**:
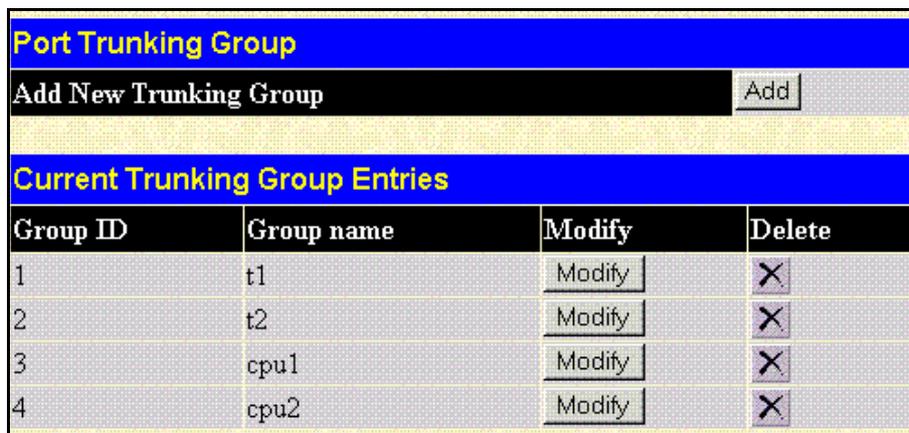
Figure 4- 7. Port Trunking Group window

To configure port trunk groups, click the **Add** button to add a new trunk group and then use the **Port Trunking Configuration** window below to set up trunk groups. To change or delete a port trunk group, click the **Modify** or **Delete** option in the **Current Trunking Group Entries** table pictured above.
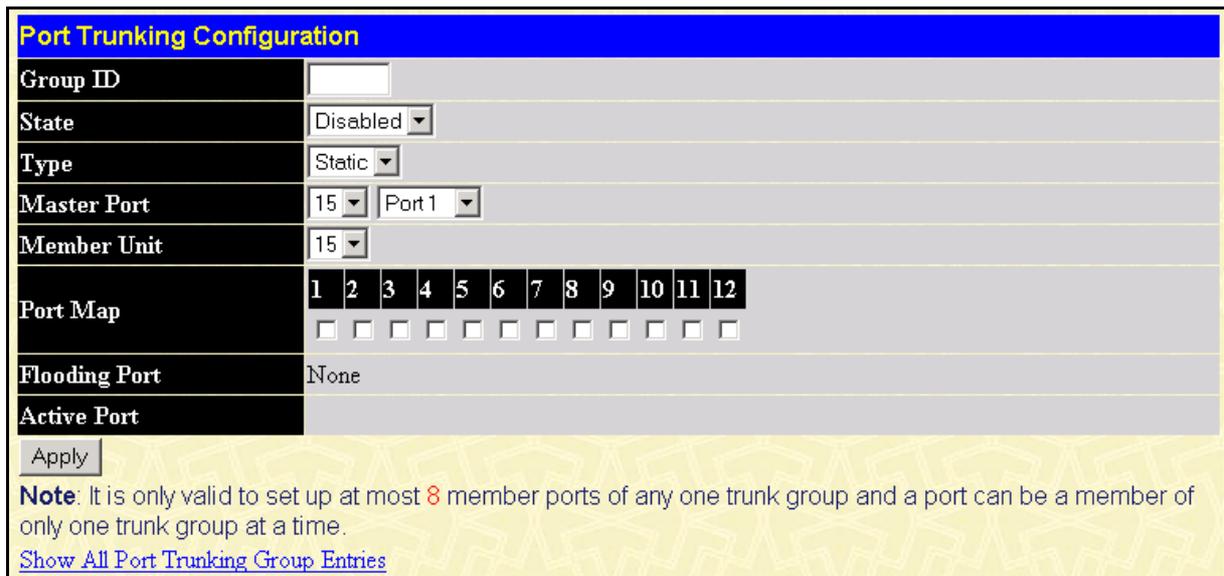
Figure 4- 8. Port Trunking Configuration window

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group.
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.
Port Map	Choose the members of the trunked group. Up to eight ports per group can be assigned to a group.
Flooding Port	A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts.
Active Port	Shows the port that is currently forwarding packets.

LACP Port Settings

The **LACP Port Mode Setup** window is used in conjunction with the Link Aggregation window to create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

Figure 4- 9. LACP Port Mode Table window

The user may set the following parameters:

Parameter	Description
Unit	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a DGS-3212SR Switch in standalone mode.
From/To	A consecutive group of ports may be configured starting with the selected port.
Mode	*Active* – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.
	Passive – LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have "active" LACP ports (see above).

After setting the previous parameters, click **Apply** to allow your changes to be implemented. The LACP Port Table shows which ports are active and/or passive.

Port Access Entity

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:
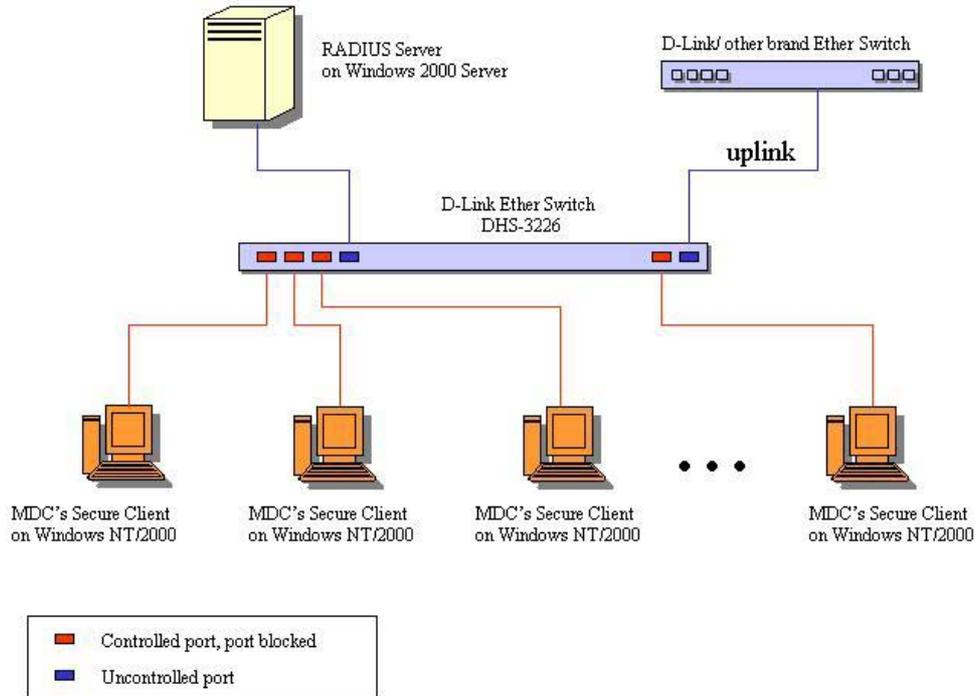

Figure 4- 10. Typical 802.1X Configuration Prior to User Authentication

Once the user is authenticated, the Switch unblocks the port that is connected to the user as shown in the next figure.
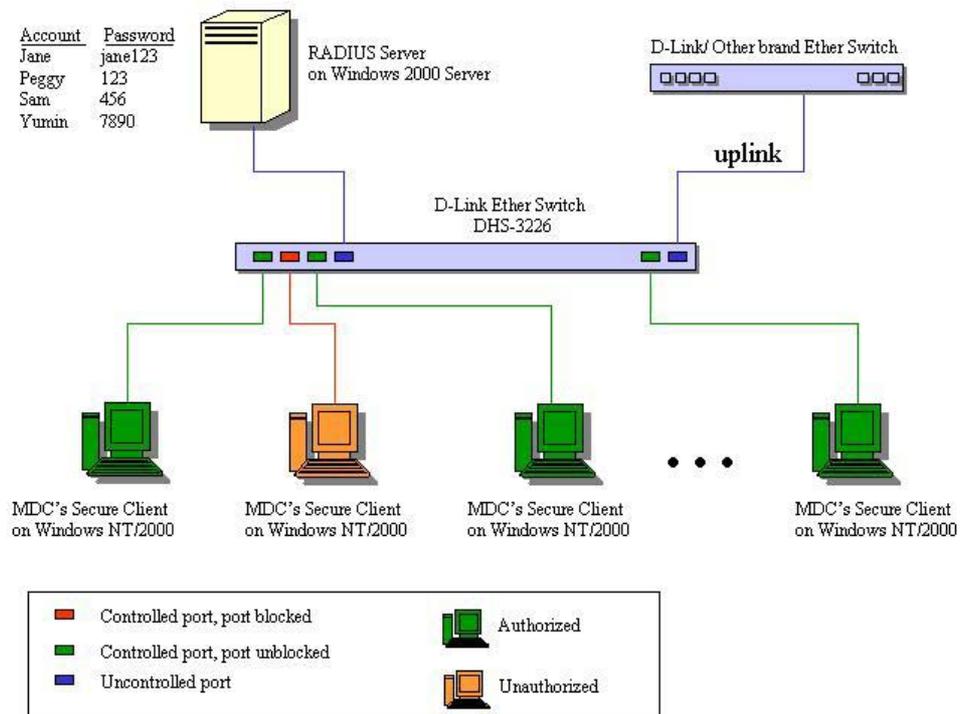
Figure 4- 11. Typical 802.1X Configuration with User Authentication

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.
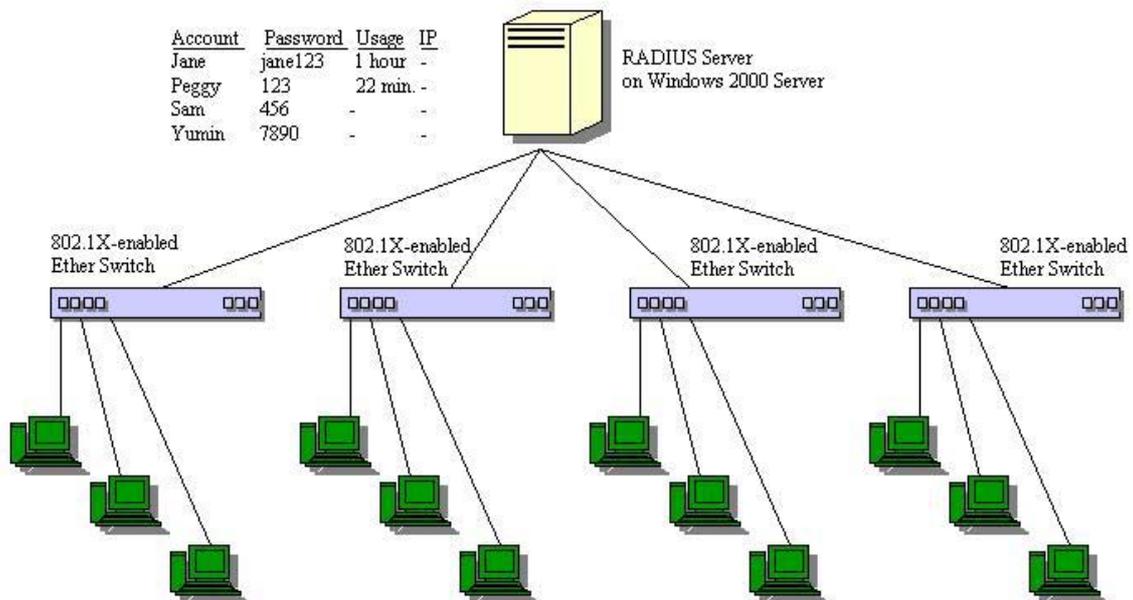
Figure 4- 12. Typical Configuration with 802.1X Fully Implemented

47

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

Table 4- 1. Conformance to IEEE 802.1X Standards

802.1X Authenticator Settings

To display the current 802.1X Authenticator Settings on the Switch, open the **Security** folder, and then the **Port Access Entity** folder and finally click on the **802.1X Authenticator Settings** link:

Unit: 15

802.1X Authenticator Settings

Port	AdmDir	PortControl	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	Auto	30	60	30	30	2	3600	no
2	both	Auto	30	60	30	30	2	3600	no
3	both	Auto	30	60	30	30	2	3600	no
4	both	Auto	30	60	30	30	2	3600	no
5	both	Auto	30	60	30	30	2	3600	no
6	both	Auto	30	60	30	30	2	3600	no
7	both	Auto	30	60	30	30	2	3600	no
8	both	Auto	30	60	30	30	2	3600	no
9	both	Auto	30	60	30	30	2	3600	no
10	both	Auto	30	60	30	30	2	3600	no
11	both	Auto	30	60	30	30	2	3600	no
12	both	Auto	30	60	30	30	2	3600	no

Figure 4- 13. 1st 802.1X Authenticator Settings window

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 second **802.1X Authenticator Settings** window, as shown below.

Figure 4- 14. 2nd 802.1X Authenticator Settings window

The following Authenticator Settings parameters can be set:

Parameter	Description
Unit	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 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	This allows you to control the port authorization state. Select *Force_authorized* 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 *Force_unauthorized* 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. If *Auto* is selected, it will enable 802.1X and cause 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. The default setting is *Auto*.

49

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.

PAE System Control

To set the port authenticating settings, open the **Security** folder, and then the **Port Access Entity** folder, and then the **PAE System Control** folder. Finally, click on the **802.1X Capability Settings** link.

802.1X Capability Settings

Figure 4- 15. 802.1X Capability Settings window

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 make your changes take effect.

Initialize Port(s)

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

Open the **Security** folder, and then the **Port Access Entity** folder, and then the **PAE System Control** folder. Finally, click on the **Initialize Port(s)** link:

Figure 4- 16. Initialize Port window

This window allows you to initialize a port or group of ports. The **Initialize Port Table** in the bottom half of the window displays the current status of the port(s) once you have clicked **Apply**.

This window displays the following information:

Parameter	Description
Unit	Allows you to specify a Switch in a switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
From/To	A consecutive group of ports may be configured starting with the selected port.
Port	The port number.
MAC Address	The MAC address of the switch where the port resides
Auth PAE State	The Authenticator PAE State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, *ForceUnauth*, and *N/A*.
Backend_State	The Backend Authentication State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize,* and *N/A.*
Oper Dir	The Operational Controlled Directions are *both* and *in.*
PortStatus	The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

Reauthenticate Port(s)

This window allows you to reauthenticate a port or group of ports. The **Reauthenticate Port Table** displays the current status of the port(s) once you have clicked **Apply**.

Open the **Security** folder, and then the **Port Access Entity** folder, and then the **PAE System Control** folder. Finally click on the **Reauthenticate Port(s)** link:

Figure 4- 17. Reauthenticate Port window

This window displays the following information:

Parameter	Description
Unit	Allows you to specify a Switch in a switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
From/To	A consecutive group of ports may be configured starting with the selected port.
Port	The port number.
MAC Address	The MAC address of the switch where the port resides
Auth State	The Authenticator State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, ForceUnauth, and *N/A*.
Backend_State	The Backend State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize,* and *N/A.*
OperDir	The Operational Controlled Directions are *both* and *in.*
PortStatus	The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

Radius Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

Radius Server

Click the **Radius Server** link in the **Radius Server** folder under **Port Access Entity** in the **Security** folder under **Configuration**.

Figure 4- 18. Authentic Radius Server Setting window

The following parameters can be set:

Parameter	Description
Succession	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.
Confirm Key	Retype the Key information from the Key field above.
Status	This drop-down menu allows you to select *Valid* or *Invalid*.

IGMP

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 Settings** window. 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.

IGMP Snooping

Use this window to view IGMP Snooping status. To modify settings, click the **Modify** button for the VLAN ID you want to change.

VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Non-Querier	Modify
2	v2	Disabled	Non-Querier	Modify
3	v3	Disabled	Non-Querier	Modify

Current IGMP Snooping Group Entries

Figure 4- 19. Current IGMP Snooping Group Entries window

Click the **Modify** button to bring up the **IGMP Snooping Settings** window pictured below.

IGMP Snooping Settings

VLAN ID	1
VLAN Name	default
Query Interval	125
Max Response Time	10
Robustness Value	2
Last Member Query Interval	1
Host Timeout	260
Route Timeout	260
Leave Timer	2
Querier State	Disabled
State	Disabled

Apply

Show All IGMP Group Entries

Figure 4- 20. IGMP Snooping Settings window

The IGMP Snooping Settings are described below:

Parameter	Description
VLAN ID	The VLAN ID number.
VLAN Name	The VLAN name.
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. The default value is *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). The default value is *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*. The default value is *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. The default value is *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. The default value is *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. The default value is *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 *Enabled* to enable transmitting IGMP Query packets. The default value is *Disabled*.
State	Select *Enabled* to implement IGMP Snooping. This is *Disabled* by default.

Static Router Ports Entry

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, and 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** window, as shown below.

Figure 4- 21. Current Static Router Port Entries window

The window 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** window, as shown below.

Figure 4- 22. Static Router Ports Settings window

To configure a static router port(s):

1. Select the Unit containing the static router port.

2. Select the Port or Ports that will become static router ports.

3. Click **Apply** to let the changes take effect.

The following parameters are listed in the Static Router Port windows.

Parameter	Description
VLAN ID (VID)	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.

Spanning Tree

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. The Comparing Port States table 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

Table 4- 2. 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.

Switch Spanning Tree 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 4- 23. Switch Spanning Tree Settings window

Configure the following system-wide STP parameters and click the **Apply** button to implement them:

Parameter	Description
Spanning Tree	This field can be toggled between *Enabled* and *Disabled* using the pull-

Status *<Disabled>*	down menu. This will enable or disable the Spanning Tree Protocol (STP), globally, for the Switch.
Bridge 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.
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.
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.
Bridge 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(1-10) *<3 >*	This is the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default value is *3*.
Forwarding BPDU *<Enabled >*	This can be *Enabled* or *Disabled*. When it is *Enabled* it allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *Enabled*.

NOTE: 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

STP Port Settings									
Unit	From	To	State	Cost	Priority	Migration	Edge	P2P	Apply
15 ▼	Port 1 ▼	Port 1 ▼	Disabled ▼	0	0	No ▼	No ▼	No ▼	Apply

The STP Port Information								
Port	Designated Bridge	State	Cost	Priority	Edge	P2P	STP Status	Role
1	N/A		*200000	Stacking Link Port				
2	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
3	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp
4	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
5	N/A		*200000	Stacking Link Port				
6	N/A		*200000	Stacking Link Port				
7	N/A		*200000	Stacking Link Port				
8	N/A		*200000	Stacking Link Port				
9	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp
10	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
11	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
12	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled

Figure 4- 24. STP Port Settings window

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 for STP port configuration:

Parameter	Description
Unit	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a DGS-3212SR 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	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	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	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	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.

Forwarding & Filtering

The Switch allows permanent or static entries into the forwarding database (FDB). These FDB entries are MAC addresses that will not age out. In addition, multicast forwarding may be customized to conform to rules for the different ports by setting up multicast filter modes for each port.

Unicast Forwarding

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

Figure 4- 25. Setup Static Unicast Forwarding Table window

To add an entry, define the following parameters:

Parameter	Description
VLAN ID	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.

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.

Multicast Forwarding

The following window describes 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 window below:
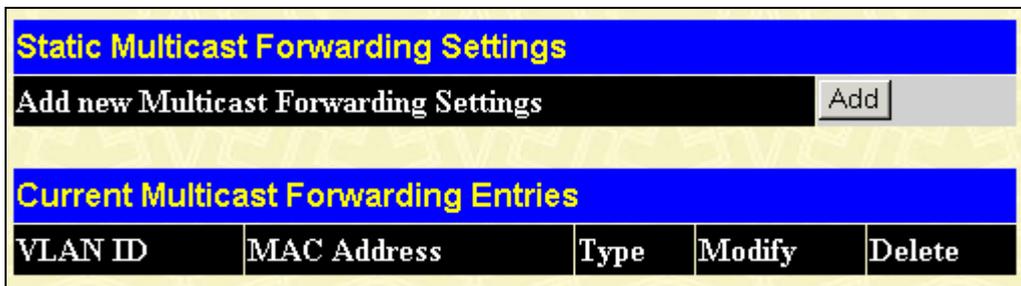
Figure 4- 26. Static Multicast Forwarding Settings window

The **Static Multicast Forwarding Settings** window 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** window, as shown below.
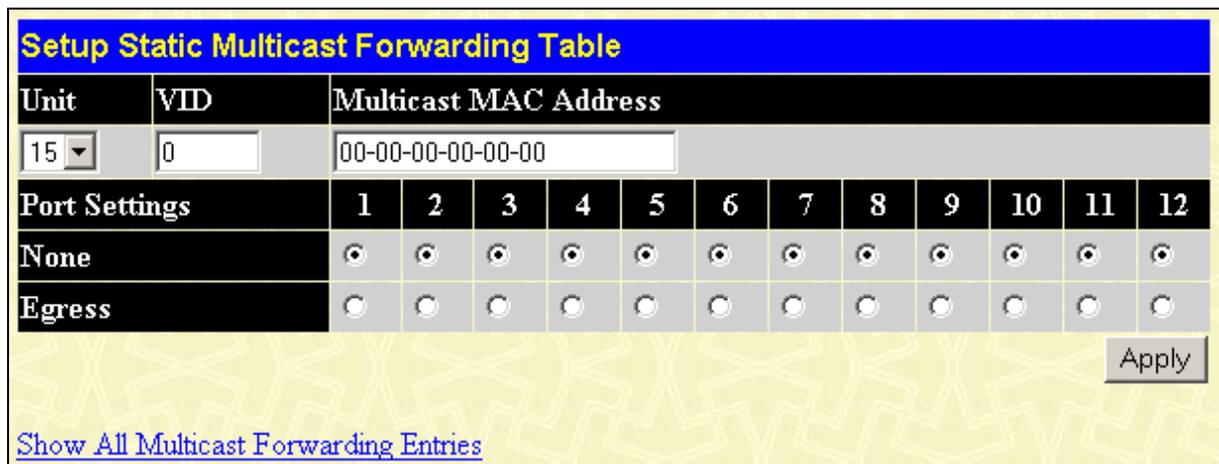
Figure 4- 27. Setup Static Multicast Forwarding Table window

The following parameters can be set:

Parameter	Description
Unit	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a DGS-3212SR Switch in standalone mode.

VID	The VLAN ID of the VLAN the MAC address below belongs to.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
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 and Egress. None means there are no restrictions on the port dynamically joining the multicast group. If None is chosen, then an end station attached to the port can join the multicast group using GMRP. Egress means the port is a static member of the multicast group.

Multicast Port Filtering Mode

The following window describes how to set up Multicast port filtering on the Switch. Open the **Forwarding & Filtering** folder and click on the **Multicast Port Filtering Mode** link to see the entry window below:

Figure 4- 28. Multicast Port Filtering Mode Setup window

The following parameters can be set:

Parameter	Description
Unit	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a DGS-3212SR Switch in standalone mode.
From/To	A consecutive group of ports may be configured starting with the selected port.

Mode	This drop-down menu allows you to select the action the switch will take when it receives a multicast packet that is to be forwarded to one of the ports in the range specified above.

Forward All Groups – Instructs the switch to forward a multicast packet to all multicast groups residing within the range of ports specified above.

Forward Unregistered Groups – Instructs the switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above.

Filter Unregistered Groups – Instructs the switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above

VLANs

The Switch Web Manager's VLANs sub-folder is divided into two main windows, **802.1Q Static VLANs** and **802.1Q Port Settings**. Each is described after a short overview of VLANs.

Understanding 802.1Q VLANs

This review of 802.1Q VLANs presents some basic background about how VLANs work according to the IEEE 802.1Q standard. VLANs operate according to the same rules regardless of whether the Switching environment is Layer 2 or Layer 3. The difference is primarily that in a Layer 3 Switch there is an added capability of unique association between a VLAN and an IP interface or subnet group.

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 DGS-3212SR 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.
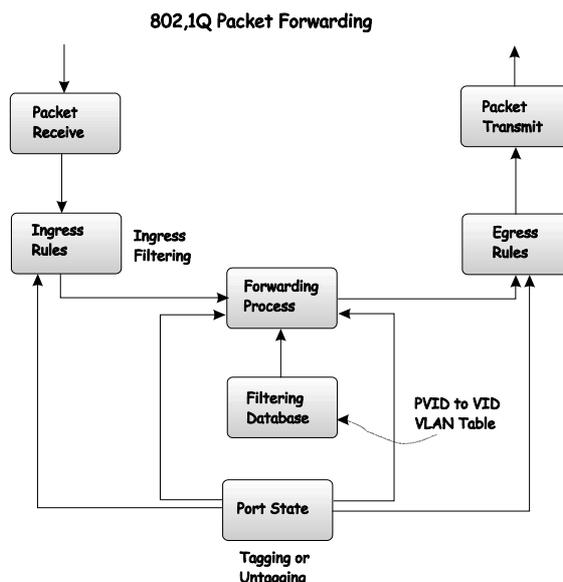
Figure 4- 29. 802.1Q Packet Forwarding

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 three bits or user priority, one bit of Canonical Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones) and twelve bits of VLAN ID (VID). The three 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 twelve bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by four octets. All of the information contained in the packet originally is retained.
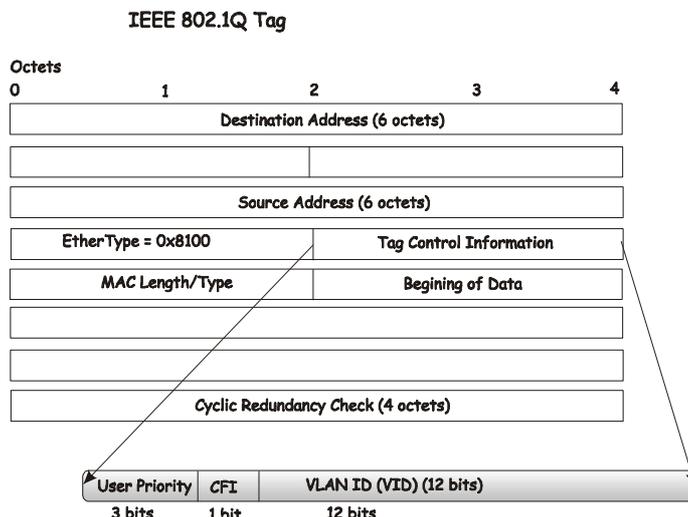
Figure 4- 30. IEEE 802.1Q Tag

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.
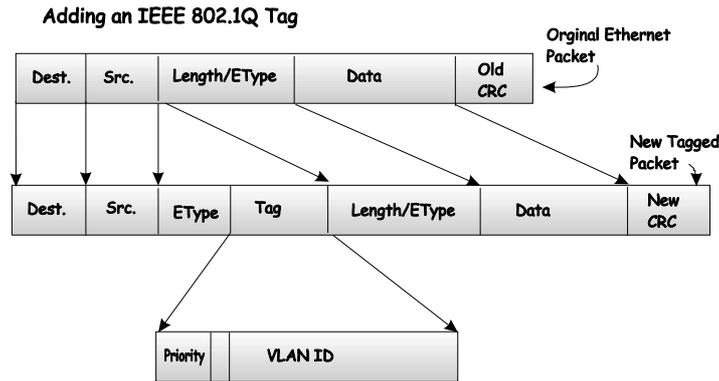
Figure 4- 31. Adding an IEEE 802.1Q Tag

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

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

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

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

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

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

Tagging and Untagging

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

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

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by

and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

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

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

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

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

802.1Q Static VLANs

To create or modify an 802.1Q VLAN:

In the **Configuration** folder, open the **VLANs** folder and click the **Static VLAN Entry** link to open the following window:
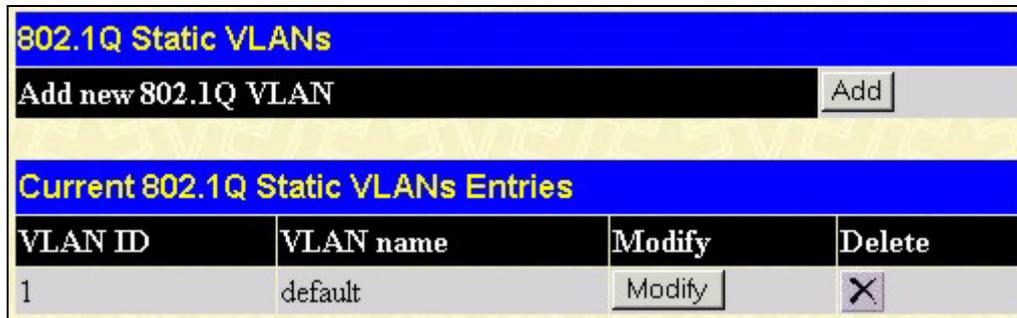
Figure 4- 32. 1st 802.1Q Static VLANs window

The first **802.1Q Static VLANs** window 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. A new window 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 window.

Figure 4- 33. 2nd 802.1Q Static VLANs window

To configure the newly created VLAN, select the Switch being configured from the **Unit** drop-down menu and provide a unique VLAN identifier and name. Configure the port settings for VLAN membership by selecting the appropriate options for each port. Click the **Apply** button to configure the VLAN port membership settings. A success or fail message appears to confirm whether the settings have been applied. To view the VLANs that have been thus far configured, click the Show All Static VLAN Entries hyperlink (see example below). To add another new VLAN entry, click the **Add** button again in the first **802.1Q Static VLANs** window.

See the table below for a description of the port VLAN membership settings.

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

Parameter	Description
Unit	Choose the Switch that the VLAN will be created on.
VID (VLAN ID)	For a new VLAN entry, type in a unique identifier. This number is used to configure other settings such as GVRP status for ports in the VLAN.
VLAN Name	For a new VLAN entry type in a unique name. This name can be used to identify the VLAN for IP interface assignment. Remember that VLAN names are case-sensitive when referring to them for other applications (such as setting up IP interfaces).
Port	Configure each individual port to be specified as member or nonmember of the VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
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	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.

The illustration below displays the port settings for a new VLAN (engineering) with a VID of 11.

Figure 4- 34. Add New Static VLAN Example window

Click the Show All Static VLAN Entries link to return to the first **802.1Q Static VLANs** window, the new VLAN entry appears listed in the current entries table.

Figure 4- 35. 802.1Q Static VLANs With Added VLAN window

To change the port settings of any listed VLAN, click the **Modify** button.

Now click the **Modify** button in the first **802.1Q Static VLANs** window for the newly created VLAN (engineering). A new window appears, use this to configure the port settings to the existing VLAN, exactly as in the add new VLAN window. Notice that the VID and name cannot be changed. If you want to change the VID or VLAN Name it will be necessary to delete the existing entry and create a new one.

Figure 4- 36. 802.1Q Static VLANs – Modify window

GVRP Setting

Open the **802.1Q Port Settings** window 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. Ingress Checking is used to limit traffic by filtering incoming packets that have a PVID does not match the PVID of the port. 802.1Q port settings are also used to determine whether the Switch will share its VLAN configuration information with GARP VLAN Registration Protocol (GVRP) enabled Switches.

The window and table below describe how to configure the 802.1Q VLAN port settings for the Switch.

Figure 4- 37. 802.1Q Port Settings window

Configure the 802.1 Port Settings:

Parameter	Description
Unit	Select the relevant Switch for configuration.
From [ ] To [ ]	Use these drop-down menus to specify the range of ports that will be included in the VLAN.
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.
Frame Type	Allows you to specify the action the Switch will take when a packet is received. If you specify *Admit_all* the Switch will receive and forward all

70

	packets to this VLAN regardless of whether or not the packet has an 802.1Q VLAN tag or not. If you specify *Tagged_only* the Switch will drop and untagged packets it receives for this VLAN.
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 window above.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is disabled by default.

QoS

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 eight 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 eight hardware queues. Therefore, the Switch must have a means of mapping the eight levels specified in the IEEE 802.1p standard to the eight hardware queues used in the Switch. This is done using the Class of Service menu explained below. Further customization of priority classification can be done with the Output Scheduling menu, also explained below.

Individual ports may still be assigned priority using the eight 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.

802.1p 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 in the **QoS** sub-folder:

Figure 4- 38. Port Default Priority assignment window

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.

802.1p User Priority

The DGS-3212SR allows the assignment of a User Priority to each of the 802.1p priorities.

Figure 4- 39. User Priority Configuration window

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

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 are 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 4- 40. QoS Output Scheduling Configuration window

Use the Scheduling Mechanism drop-down menu to select between a *RoundRobin* and a *Strict* mechanism for empting the priority queues.

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 4- 41. Traffic Segmentation Setting window

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.

Bandwidth Control

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

Figure 4- 42. Bandwidth Settings window

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. The number 15 indicates a Switch in standalone mode.
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.

MAC Notification

MAC address notification is used to monitor MAC addresses as they are learned and entered into the Switch's MAC forwarding database.

Global Settings
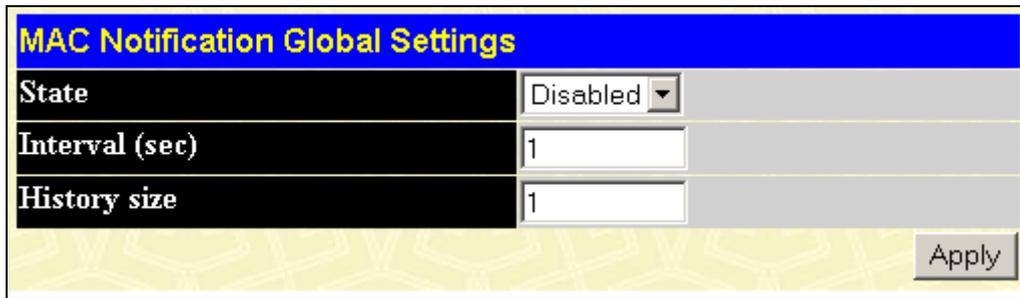
Figure 4- 43. MAC Notification Global Settings window

The following parameters can be set:

Parameter	Description
State	This drop-down menu is used to enable or disable MAC notification on the selected Switch.
Interval (sec)	The time in seconds between notifications.
History size	The maximum number of entries that will be listed in the History log. Up to *500* entries can be specified.

Port Settings

Enable or disable MAC notification for ports with the window below.

Figure 4- 44. MAC Notification Port Settings window

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. Number 15 indicates a Switch in standalone mode.
From/To	A consecutive group of ports may be configured starting with the selected port.
State	This pull-down menu allows you to enable or disable MAC notification for the specified Switch and group of ports.

System Log Server

Use the System Log to keep a record of warning and other pertinent system information.

The Switch can send system log (SysLog) messages to up to four designated servers.
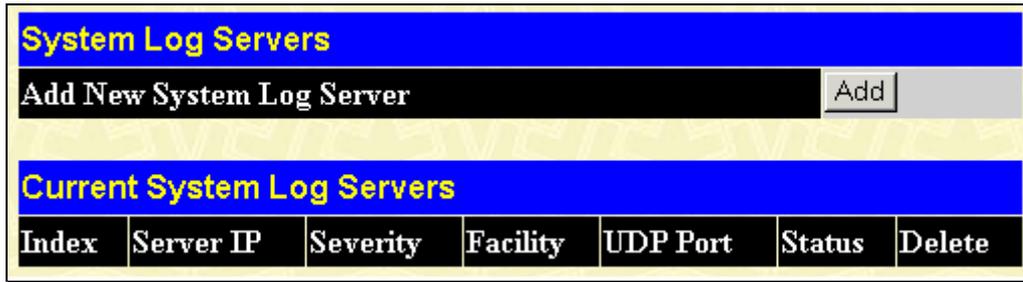
Figure 4- 45. System Log Servers window

Click the **Add** button to bring up the window pictured below. The parameters configured for adding System Log are described in the table below. To eliminate a System Log Server configuration, click the *X* in the Delete column for the configuration being removed.
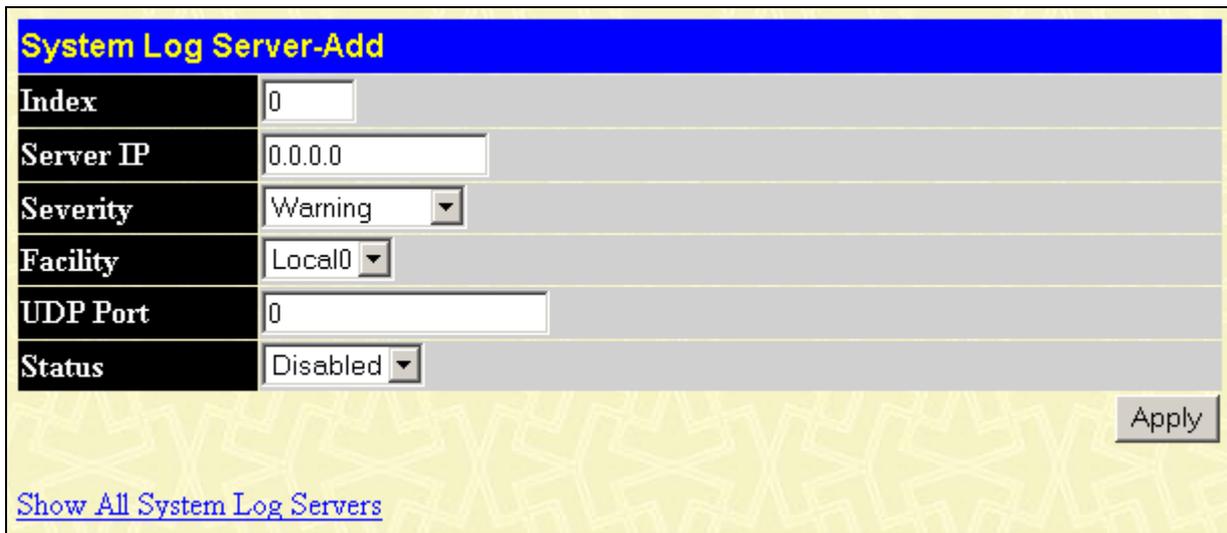
Figure 4- 46. System Log Servers – Add window

Configure these parameters for the system log:

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 supports. 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

Port Security

A given port's (or a range of port's) 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 Admin State 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 4- 47. Port Security Settings window

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. The number 15 indicates a Switch in standalone mode.
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(0-10)	The number of MAC addresses that will be in the MAC address forwarding table for the selected Switch and group of ports.
Lock Address 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 *Permanent*, *DeleteOnReset*, and *DeleteOnTimeout*.

SNTP Setting

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

Time Setting

Figure 4- 48. Current Time: Status window

The following parameters can set or are displayed:

Parameter	Description
Current 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 Secondary Server	This is the primary server the SNTP information will be taken from
SNTP Poll Interval in Seconds	This is the interval between requests for updated SNTP information.
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 4- 49. Time Zone and DST Settings window

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 Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will 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 Week of the month	Enter the week of the month that DST will start.
From: Which Day of Week	Enter the day of the week that DST will start on.
From: Which Month	Enter the month DST will start on.
From: What Time HH:MM	Enter the time of day that DST will start on.
To: Which Week	Enter the week of the month the DST will end.
To: Which Day	Enter the day of the week that DST will end.
To: Which Month	Enter the month that DST will end.
To: What Time HH:MM	Enter the time DST will end.
DST Annual Settings	Annual - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.
From: What Month	Enter the month DST will start on, each year.
From: What Date	Enter the day of the week DST will start on, each year.
From: What Time	Enter the time of day DST will start on, each year.
To: What Month	Enter the month DST will end on, each year.
To: What Date	Enter the day of the week DST will end on, each year.
To: What Time	Enter the time of day that DST will end on, each year.

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** window, as shown below.

Figure 4- 50. Access Profile Table window

To add an entry to the **Access Profile Table** window, click the **Add** button. This will open the **Access Profile Configuration** window, as shown below. There are two **Access Profile Configuration** windows − 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** windows by using the Type drop-down menu, and clicking on the **Apply** button. The **Access Profile Configuration** window for Ethernet is shown below.

Access Profile Configuration

Profile ID(1-255)	1
Type	Ethernet ▾
Vlan	☐
Source Mac	☐ 00-00-00-00-00-00
Destination Mac	☐ 00-00-00-00-00-00
802.1p	☐
Ethernet type	☐
Mode	☐ ⦿ Permit ○ Deny
	Apply

Show All Access Profile Table Entries

Figure 4- 51. Access Profile Configuration (Ethernet) window

The following parameters can be set:

Parameter	Description
Profile ID(1-255)	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* to *255*.
Type	Select profile based on Ethernet (MAC Address) or IP address. This will change the window 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 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	Selecting this option instructs the Switch to examine the Ethernet type value of each packet header and use this as the, or part of the criterion for forwarding.

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.

The page shown below is the **Access Profile Configuration** window for IP:

Figure 4- 52. Access Profile Configuration (IP) window

The following parameters can be set:

Parameter	Description
Profile ID(1-255)	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* to *255*.
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 code 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, a destination port mask or a flag bite.
	• *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).
	• *flag bit* – Specify a flag bite in the TCP header.
	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 TCP 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.

To establish the rule for a previously created Access Profile, select the Access Profile entry from the **Access Profile Table** window and then click the **Modify** button for that individual entry.

Figure 4- 53. Access Rule Table window

To create a new rule set for the access profile, click the **Add** button. A new window is displayed. To remove a previously created rule, select it and click the **Delete** button.

Figure 4- 54. Access Rule Configuration (Ethernet) window

Configure the Access Rule Configuration settings on the window above.

The following parameters can be set:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Access ID	Type in a unique identifier number for this access. This value can be set from *1* to *255*.
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.

87

Priority(0-7)	Specify the priority tag, located in the packet header that will be identified by the Switch.
Replace Dscp(0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Vlan Name	Allows the entry of a name for a previously configured VLAN.
Source Mac	Source MAC Address - Enter a MAC Address for the source MAC address.
Destination Mac	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.
802.1p(0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from *a-f* and from *0-9999.*

Figure 4- 55. Access Rule Configuration (IP) window

Configure the Access Rule Configuration settings on the window above.

The following parameters can be set:

Parameter	Description
Profile ID	This is the identifier number for this profile set.

Access ID	Type in a unique identifier number for this access. This value can be set from *1* to *255*.
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.
Priority(0-7)	Specify the priority tag, located in the packet header that will be identified by the Switch.
Dscp(0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Vlan Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address - Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address- Enter an IP Address mask for the destination IP address.
Dscp(0-63)	This field allows the user to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. The user may choose a value between *0* and *63*.
Protocol	This field allows the user to modify the protocol used to configure the Access Rule Table window; depending on which protocol the user has chosen in the Access Profile Table window.

Chapter 5

Security

Trusted Host

Trusted Host

The **Security IP Management** window 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.

Figure 5- 1. Security IP Management window

The following fields can be set:
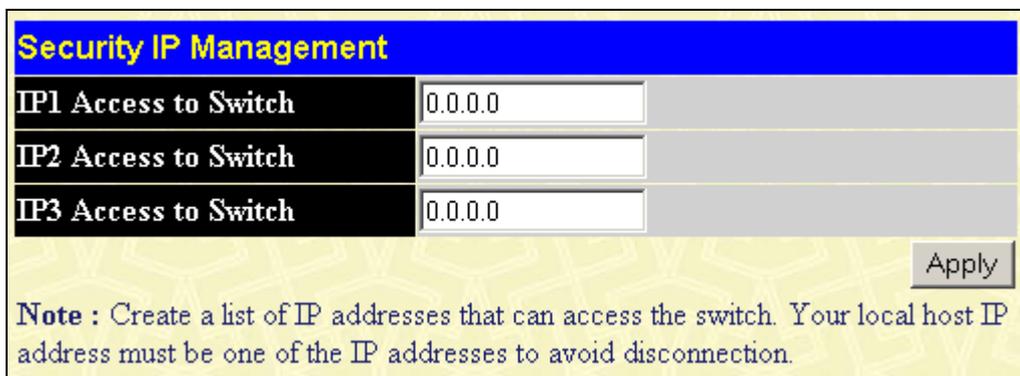
Parameter	Description
IP1 Access to Switch	Enter the IP address of a management station that will be used to manage the Switch. This IP address must be on the same subnet as the Switch.
IP2 Access to Switch	Enter the IP address of a management station that will be used to manage the Switch. This IP address 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.

Chapter 6

Management

> ***User Accounts***
> ***SNMPV3***
> ***SNMP User Table***
> ***SNMP View Table***
> ***SNMP Group Table***
> ***SNMP Community Table***
> ***SNMP Host Table***
> ***SNMP Engine ID***

User Accounts

Use the **User Account Management** to control user privileges. To view existing User Accounts, open the **Management** folder and click on the **User Accounts** link. This will open the **User Account Management** window, as shown below.
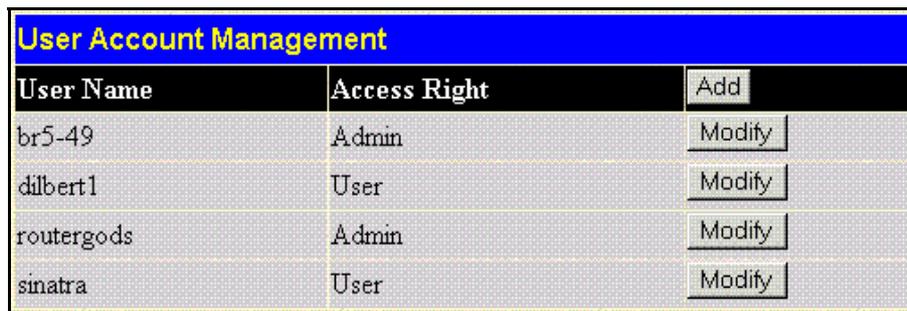
Figure 6- 1. User Account Management window

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.
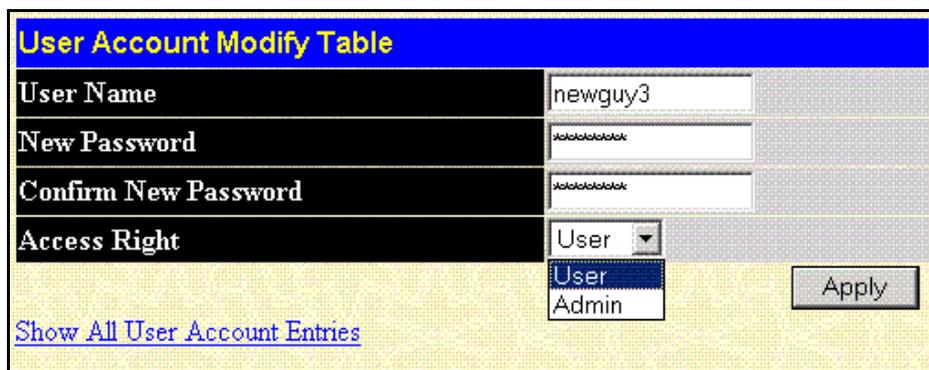
Figure 6- 2. User Account Modify Table window

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.

Figure 6- 3. User Account Modify Table window

Modify or delete an existing user account in the **User Account Modify Table** window. 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.

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

Table 6- 1. Admin and User Privileges

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

SNMPV3

The DGS-3212SR 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 windows to select the SNMP version used for specific tasks.

The DGS-3212SR 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 windows 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 **Security IP Management** window (located in the **Security** folder under **Trusted Host**).

SNMP User Table

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

Open the **Management** folder and then the **SNMPV3** folder. Finally click on the **SNMP User Table** link. This will open the **SNMP User Table**, as shown below.

Figure 6- 4. SNMP User Table window

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.

SNMP User Table Display

To display the detailed entry for a given user, click on the blue **User Name**. This will open the **SNMP User Table Display** window, as shown below.
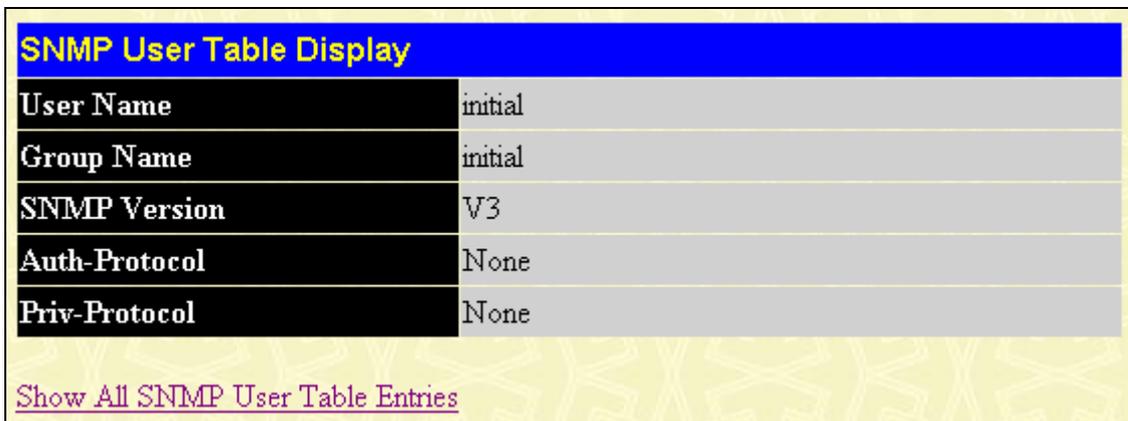
Figure 6- 5. SNMP User Table Display window

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** window. This will open the **SNMP User Table Configuration** window, as shown below.

SNMP User Table Configuration

Figure 6- 6. SNMP User Table Configuration window

The following parameters can 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 V3 Encryption	Check this to specify that SNMP version 3 will be used.
Auth-Protocol	*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 6- 7. SNMP View Table window

To delete an existing **SNMP View Table** entry, click the *X* button listed under **Delete** on the far left that corresponds to the listed View Name. To create a new entry, click the **Add** button, a separate window will appear.

SNMP View Table Configuration

Figure 6- 8. SNMP View Table Configuration window

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

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** window) to the views created in the previous window.

Figure 6- 9. SNMP Group Table window

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

SNMP Group Table Display

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

Figure 6- 10. SNMP Group Table Display window

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** window. This will open the **SNMP Group Table Configuration** window, as shown below.

SNMP Group Table Configuration

Figure 6- 11. SNMP Group Table Configuration window

The following parameters can be 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.
	SNMPv3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	*NoAuthNoPriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.
	AuthNoPriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.
	AuthPriv – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

SNMP Community Table

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

An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.

An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community.

Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

Figure 6- 12. SNMP Community Table Configuration window

The following parameters can set:

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

SNMP Host Table

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

Open the **Management** folder, and then the **SNMPV3** folder. Finally, click on the **SNMP Host Table** link. This will open the **SNMP Host Table** window, 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.
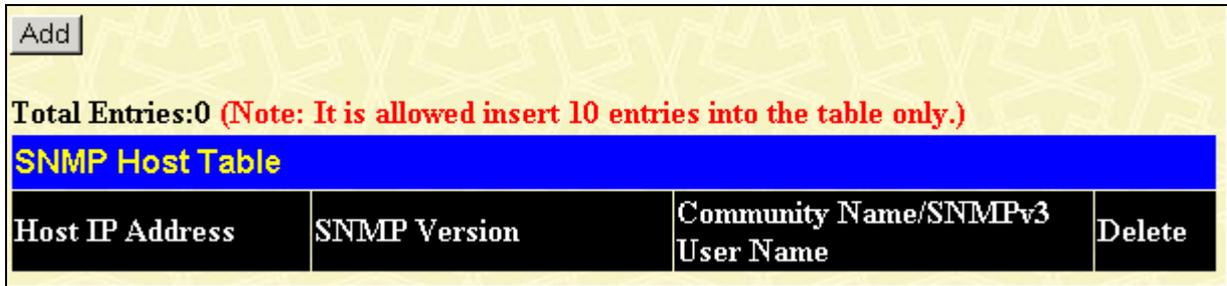

Figure 6- 13. SNMP Host Table window

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** window. This will open the **SNMP Host Table Configuration** window, as shown below.

SNMP Host Table Configuration
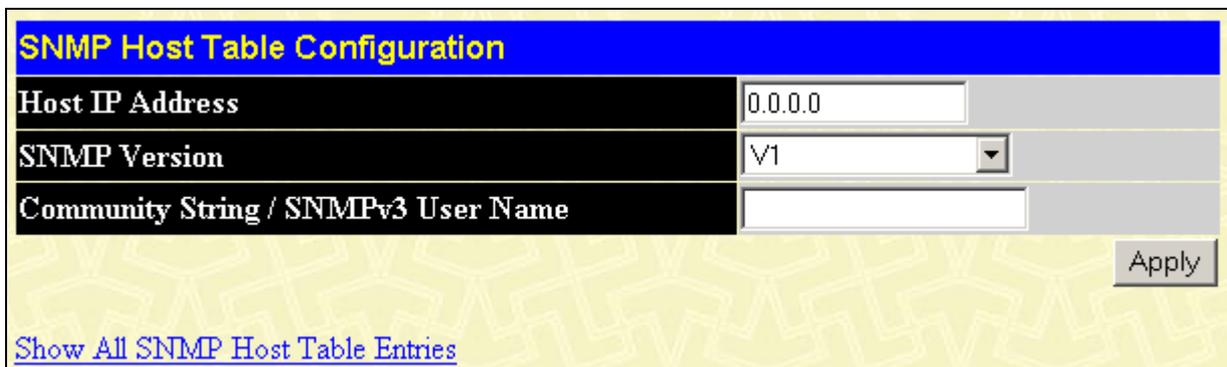
Figure 6- 14. SNMP Host Table Configuration window

The following parameters can 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* – Specifies that SNMP version 1 will be used.
	V2c – Specify that SNMP version 2c will be used.
	V3-NoAuth-NoPriv – Specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.
	V3-Auth-NoPriv – Specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.
	V3-Auth-Priv – Specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

SNMP Engine ID

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

To display the Switch's SNMP Engine ID, open the **Management** folder, and then the **SNMPV3** folder. Finally, click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID Configuration** window, as shown below.
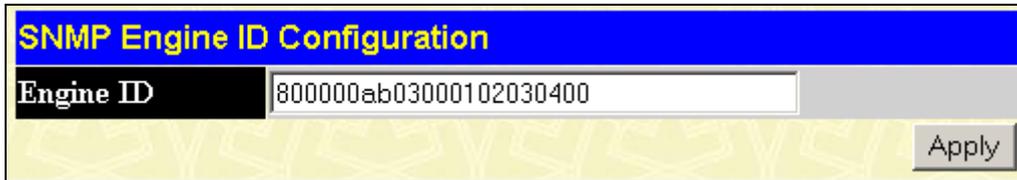

Figure 6- 15. SNMP Engine ID Configuration window

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

<div style="text-align: right; border: 1px solid black; display: inline-block;">

Chapter 7

</div>

Monitoring

> *Stack Information*
> *Port Utilization*
> *Packets*
> *Received (RX)*
> *UMB_cast (RX)*
> *Transmitted (TX)*
> *Errors*
> *Received (RX)*
> *Transmitted (TX)*
> *Size*
> *Packet Size*
> *MAC Address*
> *Switch History*
> *IGMP Snooping*
> *Browse Router Port*
> *VLAN Status*
> *Session Table*
> *Authenticator State*

The DGS-3212SR provides extensive network monitoring capabilities that can be viewed from the **Monitoring** folder.

Stack Information

The DGS-3212SR Switch can be used as a standalone high-capacity Switch or be used in a stacked arrangement. There are two hardware requirements to use the Switch in a stacked group:

1. The proper module(s) must be installed. One or two DEM-540 Stacking modules must be installed in order to use the Switch in a stacked configuration.

2. Slave Switch units in a stacked Switch group must be uniform in type and model, furthermore they must be one of the Switch models intended for use with the DGS-3212SR, namely the DES-3226S Switches.

One stacking module can be installed to stack up to four additional slave Switch units or two modules can be installed to stack up to eight additional slave Switch units.

The web manager can be used to enable or disable the stacking mode and to enable stacking for any of the built-in combination ports.

The Switch stack displayed in the upper right-hand corner of your web-browser is a virtual representation of the actual stack (see example below). The icons appear in the same order as their respective Switches.

When the Switches are properly interconnected, information about the resulting Switch stack is displayed in the **Stack Mode Setup** window. To view stacking information or to enable/disable the stacking mode, click the **Stack Information** link in the **Configuration** folder.

Stack Mode Setup	
Stack Topology	Auto Detect
Setting	MASTER
Current	MASTER
Stack Mode State	Enable ▼
Stack Port	1 2 3 4 5 6 7 8 9 10 11 12 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Apply

Total Entries : 1

Stack Information Table

ID	MAC Address	Port Range	Mode	Version	RPS Status	Model Name
15	00-22-08-33-13-00	1-12	MASTER	2.00-B09	Not Present	DGS-3212SR

Figure 7- 1. Stack Mode Setup (stacking disabled) window

To enable the stacking mode, follow the steps listed below.

1. Select *Enabled* from the Stack Mode State drop-down menu.

2. Click on the **Apply** button.

To enable stacking for one or more built-in combination ports, do the following:

1. Select *Enabled* from the Stack Mode State drop-down menu.

2. Select the Stack Port by clicking to check a corresponding selection box.

The Stack Information Table displays the read-only information listed in the table on the next page.

The current order in the Switch stack is also displayed on the front panel of each slave Switch, under the STACK NO. heading. The Stack ID LED display on the front panel of the DGS-3212SR will always display an F (15 in hex), regardless of whether the DGS-3212SR is the master Switch in a Switch stack or in standalone mode.

Below is an example of the **Stack Mode Setup** window with stacking mode enabled on Ports 9-12.

Figure 7- 2. Stack Mode Setup (stacking enabled) window

Variables in this window are described below:

Parameter	Description
ID	Displays the Switch's order in the stack. The Switch with a unit id of 1 is the master Switch.
MAC Address	Displays the unique address of the Switch assigned by the factory.
Port Range	Displays the total number of ports on the Switch. Note that the stacking port is included in the total count.
Mode	Displays the method used to determine the stacking order of the Switches in the Switch stack.
Version	Displays the version number of the stacking firmware.
RPS Status	Displays the status of an optional Redundant Power Supply.
Model Name	Displays the model name of the corresponding Switch in a stack.

When the stacked group is connected and properly configured, the virtual stack appears in the upper right-hand corner of the web page.

Figure 7- 3. Stack Information web page

Port Utilization

The **Port Utilization** window displays the percentage of the total available bandwidth being used on the port.

To view the port utilization, click on the **Monitoring** folder and then the **Port Utilization** link:
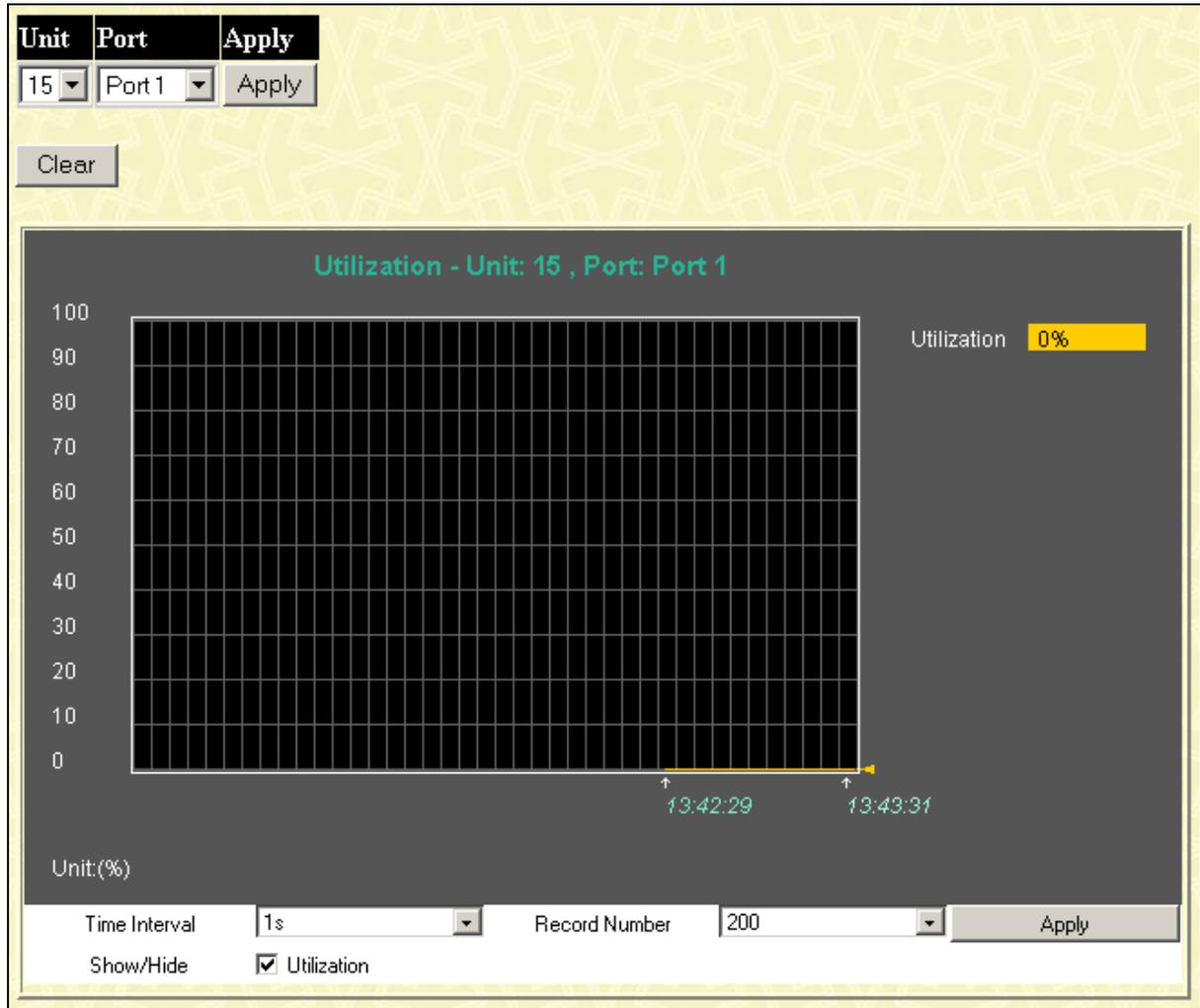
Figure 7- 4. Utilization window

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. The number 15 indicates a Switch in standalone mode.
Port	Allows you to specify a port to monitor from the Switch selected above.
Clear	Clicking this button clears all statistics counters on this window.
Time Interval *<1s>*	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number *<200>*	Select number of times the Switch will be polled between *20* and *200*. The default value is *200.*
Show/Hide	Check to display Utilization.

Packets

Various statistics can be viewed as either a line graph or a table:

- **Received Packets**
- **Received Unicast/Multicast/Broadcast Packets**
- **Transmitted Packet**

Received Packets
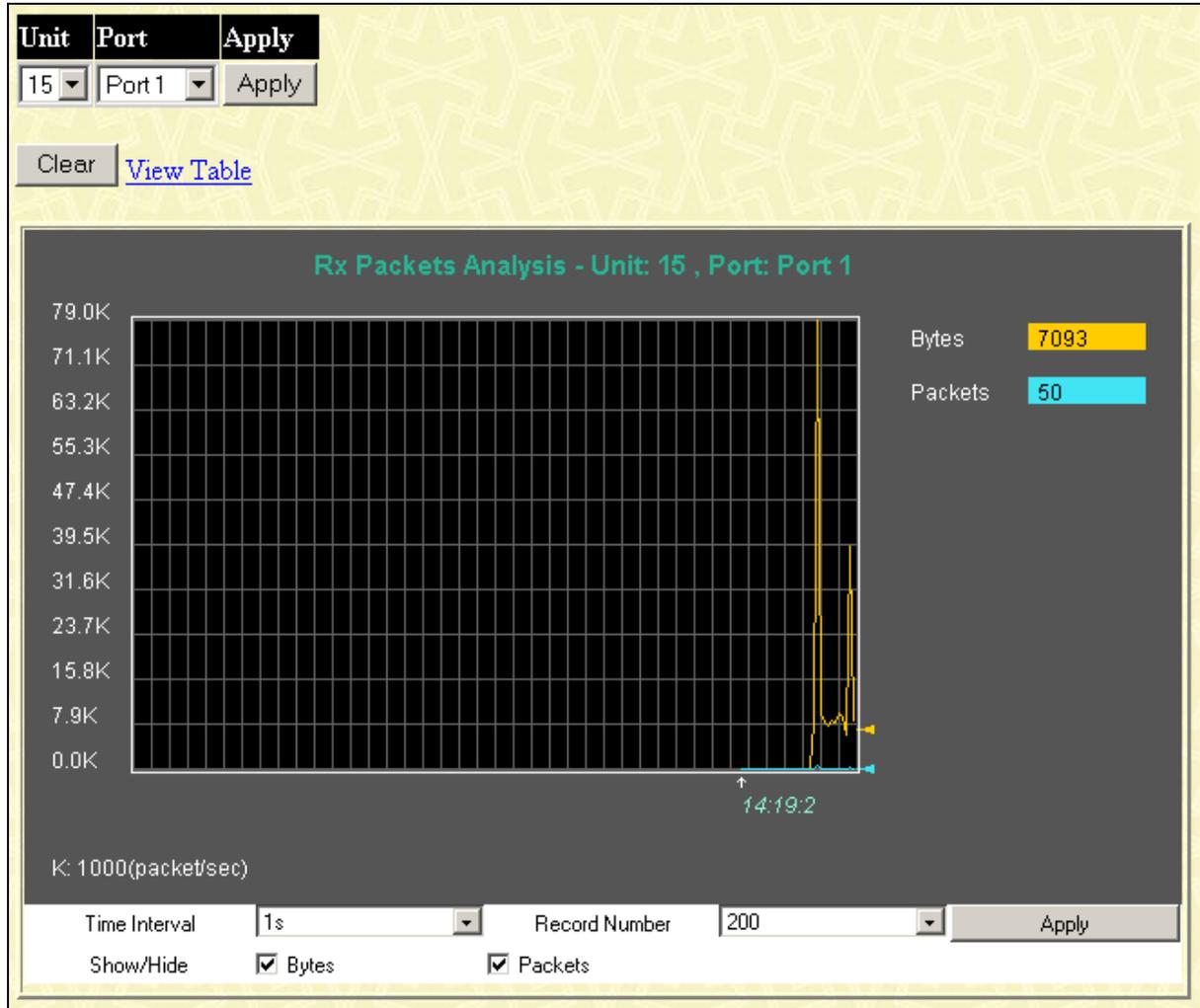
Figure 7- 5. Rx Packets Analysis (line graph for Bytes & Packets) window
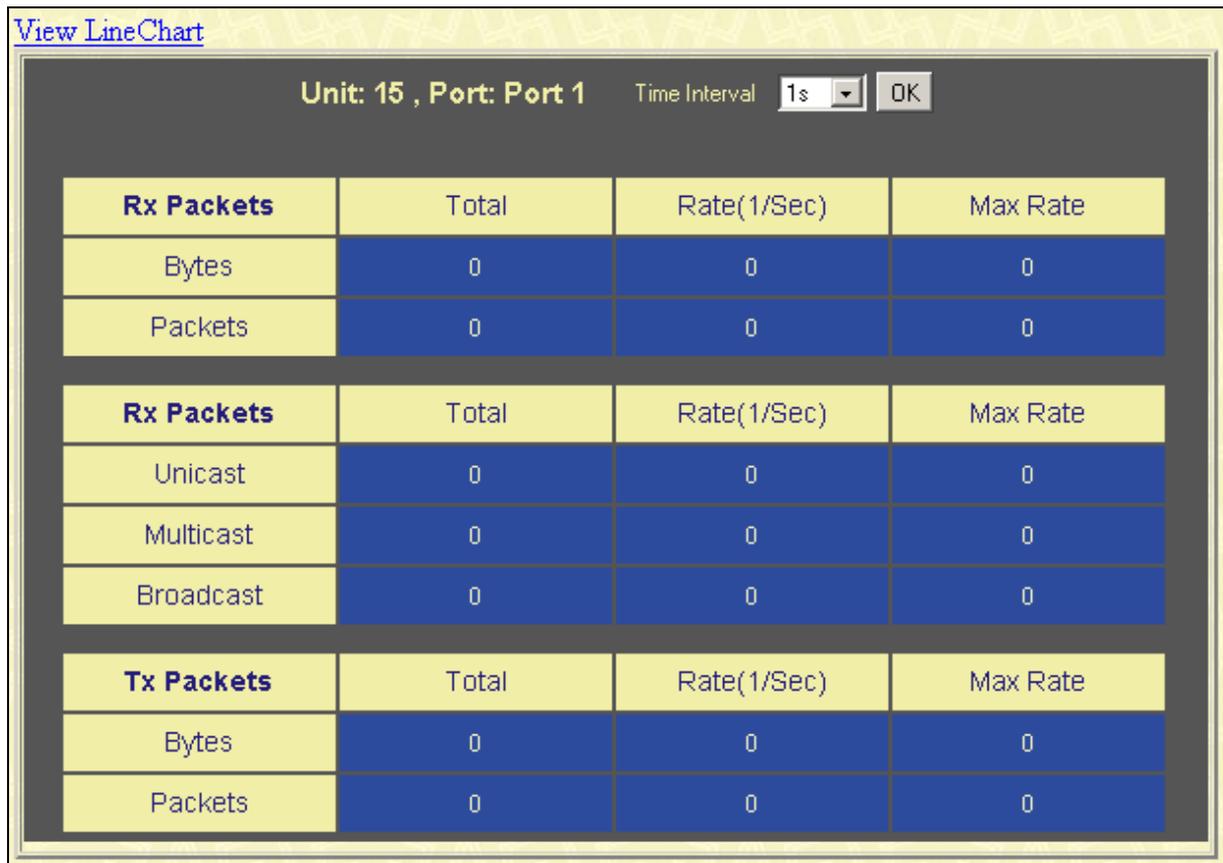
Figure 7- 6. Rx Packets Analysis (table for Bytes & Packets) window

Select the desired Switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Time 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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Time Interval *<1s>*	The time between updates received from the Switch, in seconds. The default is *1s*.
Record Number *<200>*	Select number of times the Switch will be polled between *20* and *200*. The default value is *200.*

Show/Hide   Check whether to display Bytes and Packets.

# Received Unicast/Multicast/Broadcast Packets
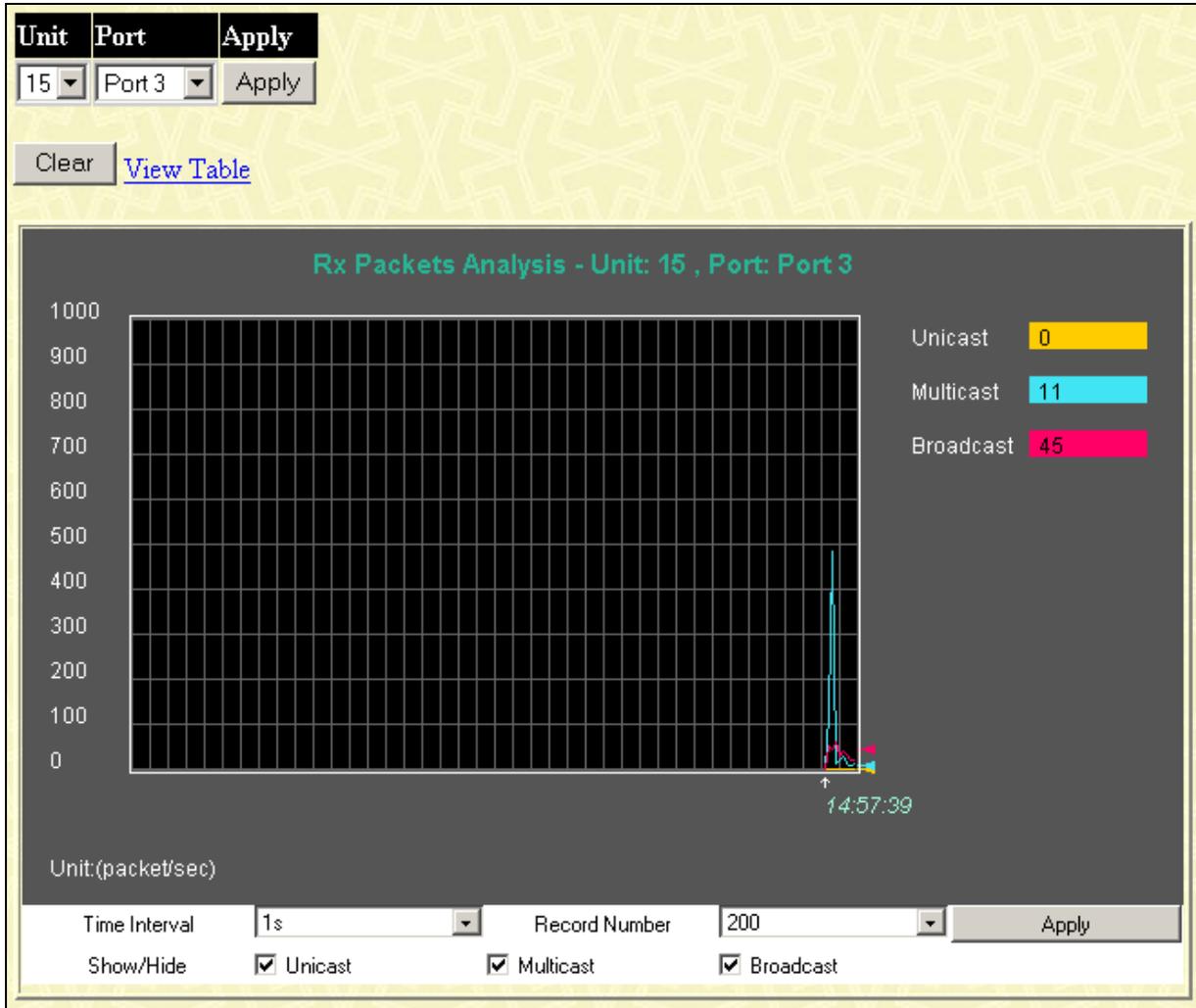
Figure 7- 7. Rx Packets Analysis (line graph for Unicast, Multicast, & Broadcast) window
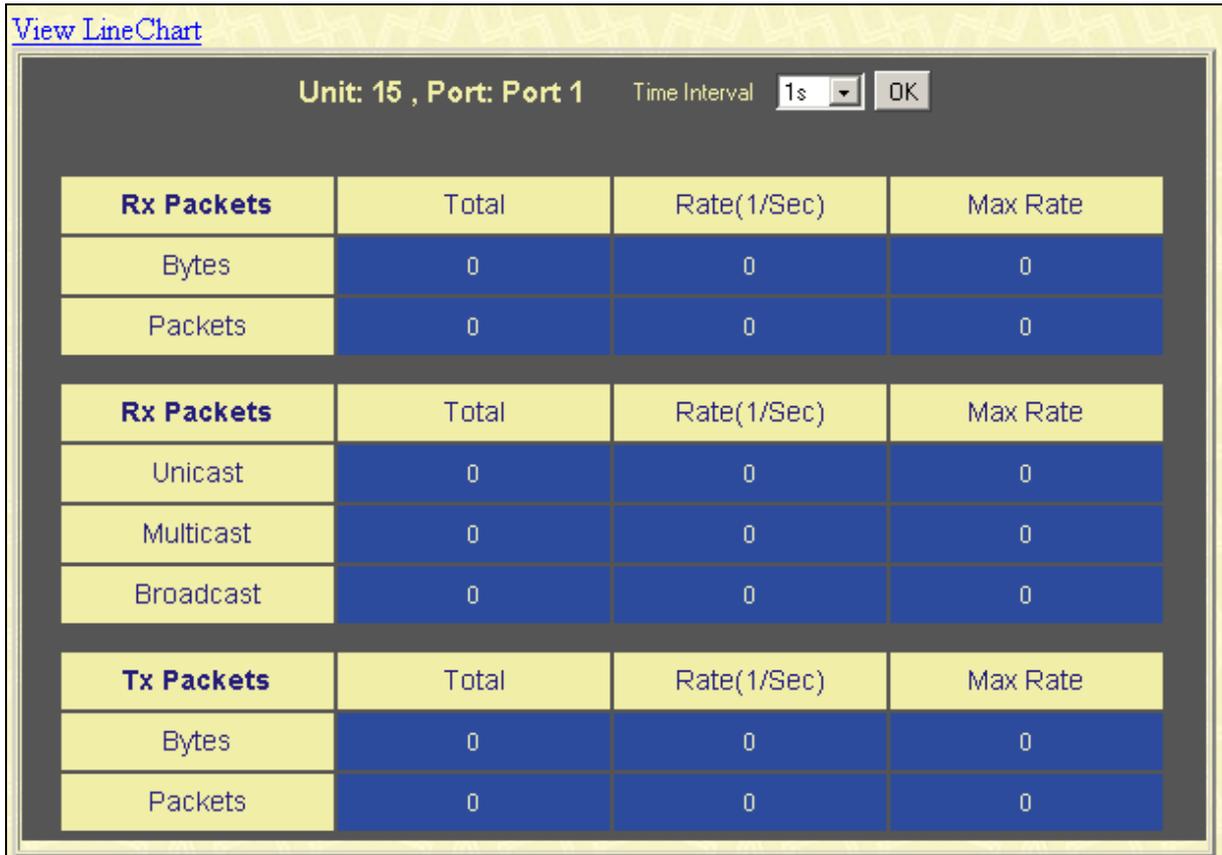
Figure 7- 8. Rx Packets Analysis (table for Unicast, Multicast, & Broadcast) window

Select the desired Switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The T**ime 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. The number 15 indicates a Switch in standalone mode.
Port	Allows you to specify a port to monitor – from the Switch selected above.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.

|	
Time Interval <*1s*>	The time between updates received from the Switch, in seconds. The default is *1s*.
Record Number <*200*>	Select number of times the Switch will be polled between *20* and *200*. The default value is *200.*
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.

Transmitted Packets
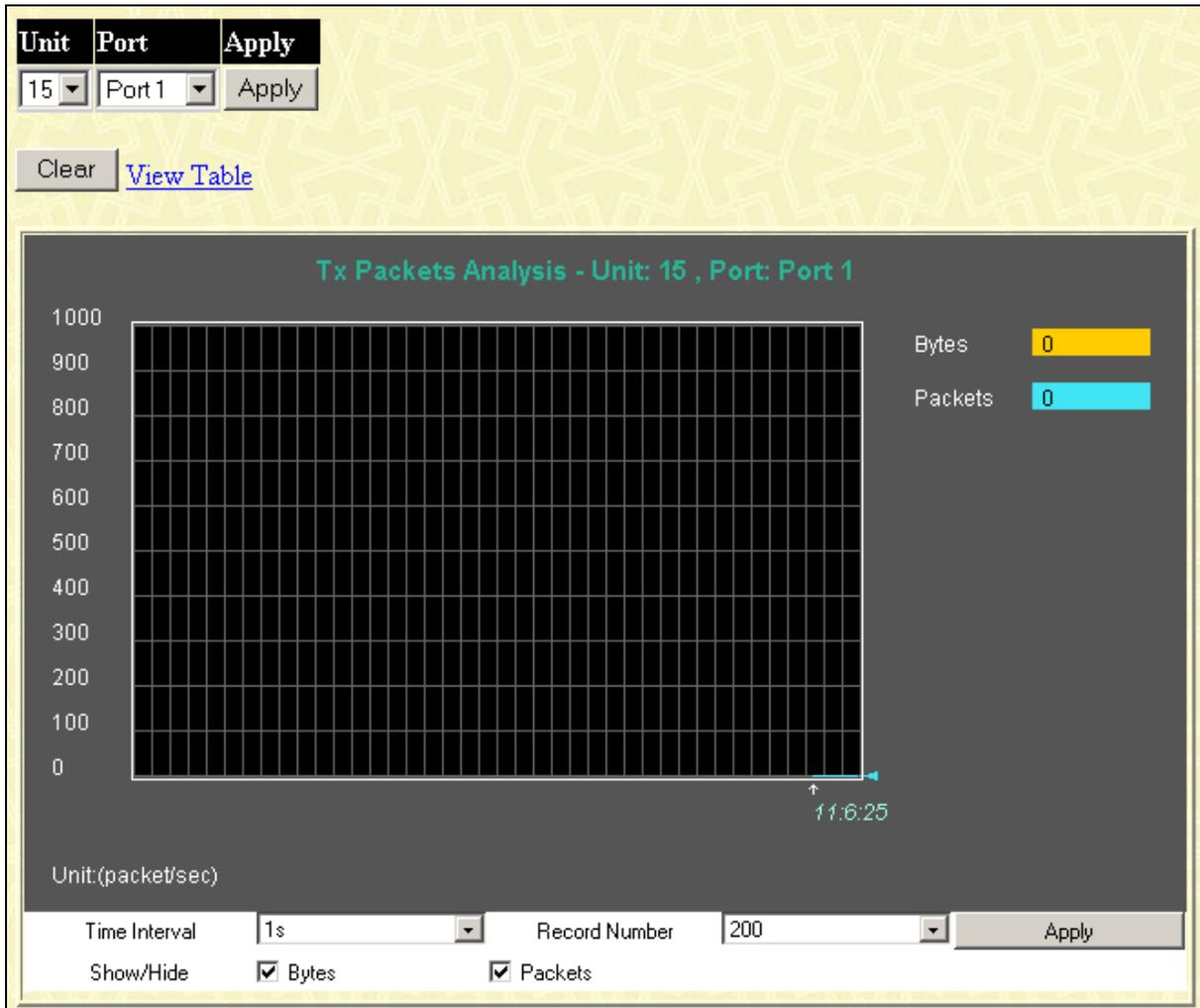
Figure 7- 9. Tx Packets Analysis (line graph for Bytes & Packets) window
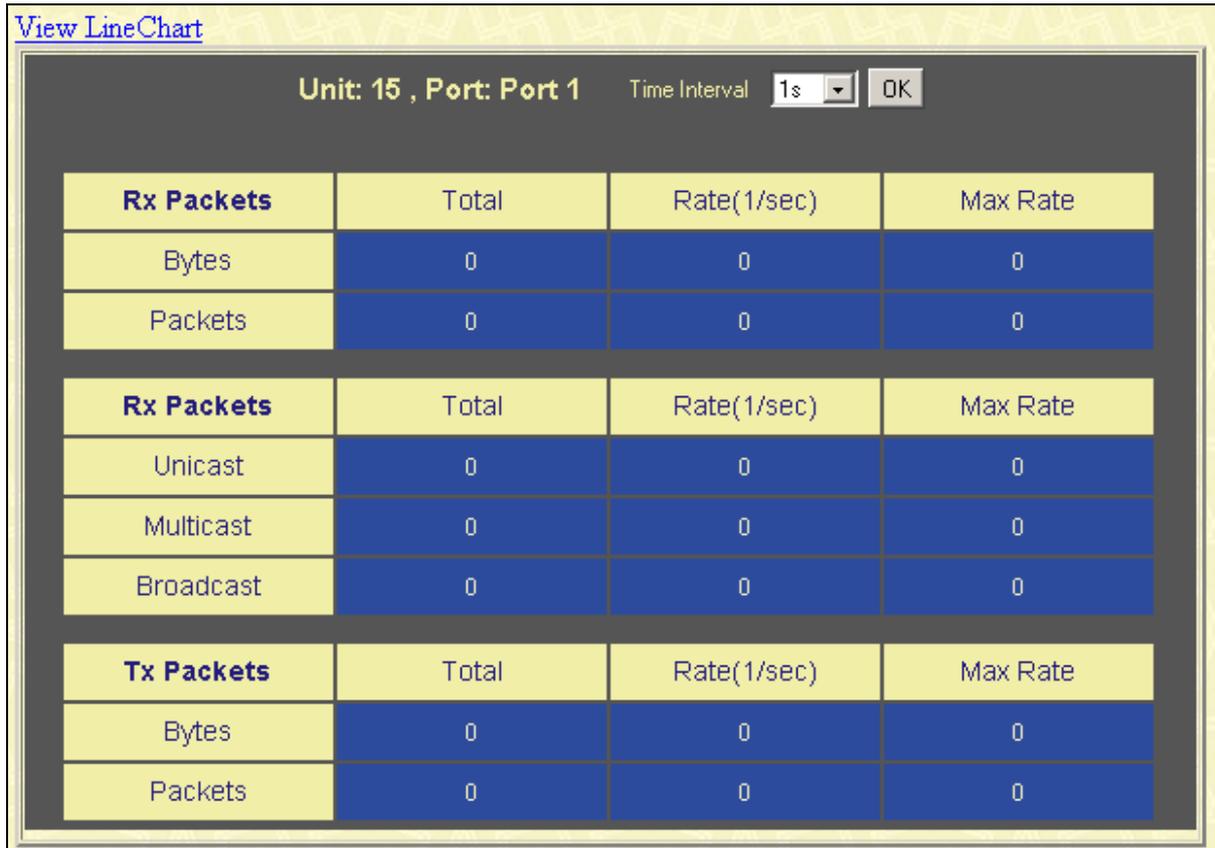
Figure 7- 10. Tx Packets Analysis (table for Bytes & Packets) window

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

The following fields 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. The number 15 indicates a Switch in standalone mode.
Port	Allows you to specify a port to monitor – from the Switch selected above.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.
Bytes	Counts the number of bytes successfully sent from the port.
Packets	Counts the number of packets successfully sent on the port.
Time Interval *<1s>*	The time between updates received from the Switch, in seconds. The default is *1s*.
Record Number *<200>*	Select number of times the Switch will be polled between *20* and *200*. The default value is *200.*

Show/Hide	Check whether to display Bytes and Packets.

Errors

Various statistics can be viewed as either a line graph or a table:

- **Received Errors**
- **Transmitted Errors**

Received Errors
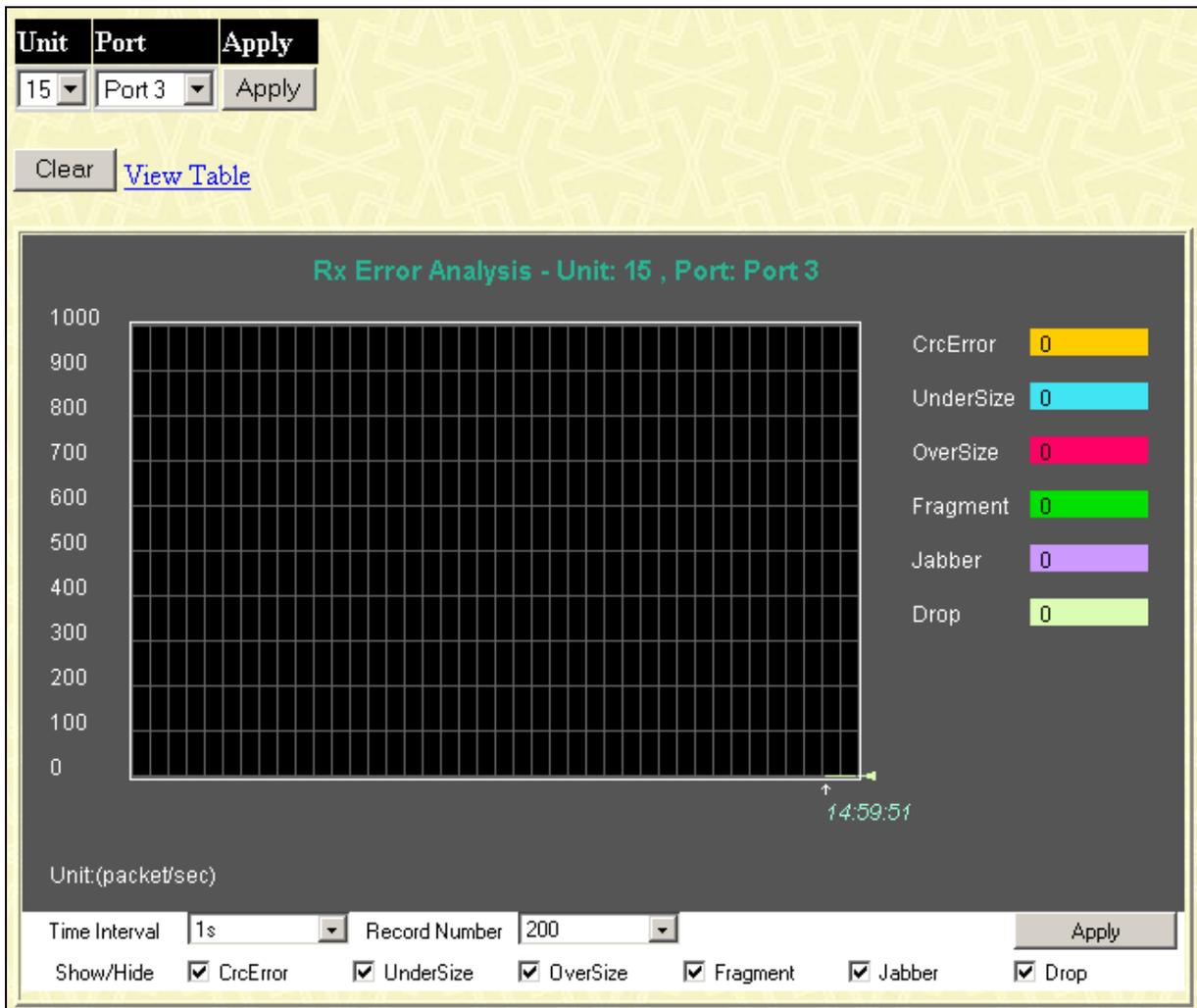
**Figure 7- 11. Rx Error Analysis (line graph) window**
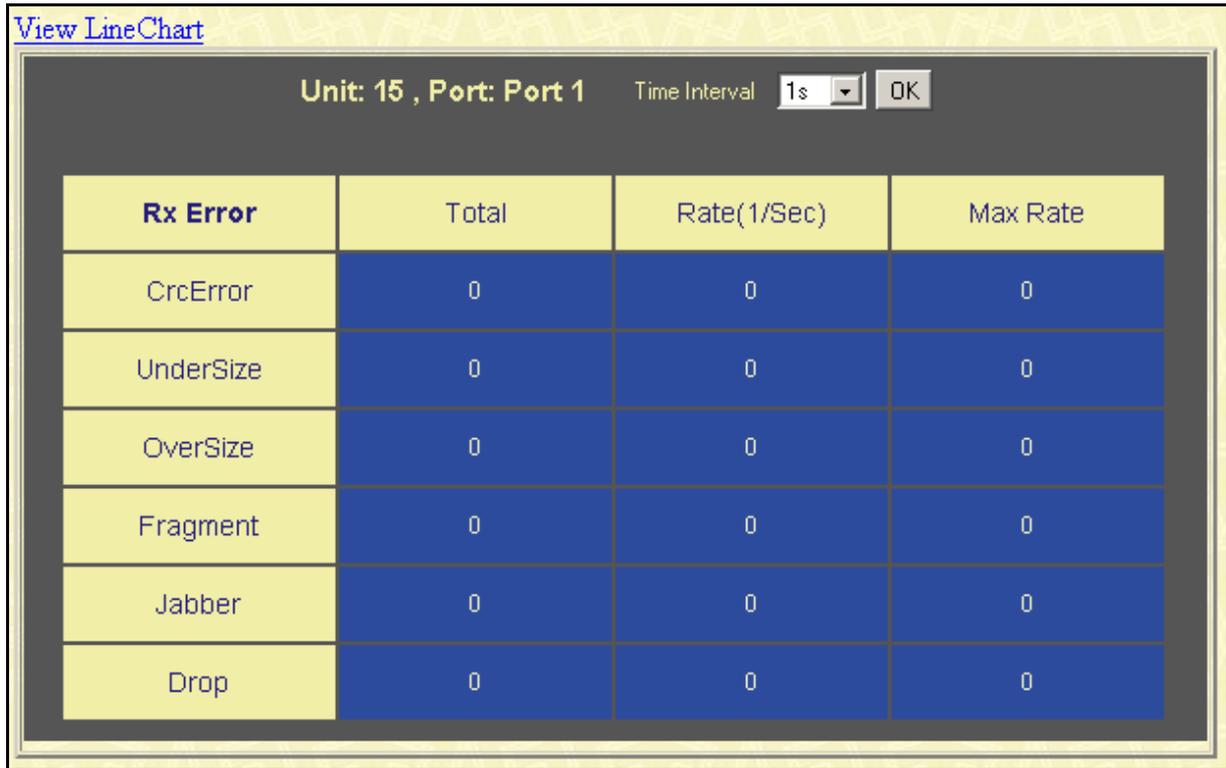
Figure 7- 12. Rx Error Analysis (table) window

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

The following fields 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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.
CrcError	Counts otherwise valid frames that did not end on a byte (octet) boundary.
UnderSize	The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
OverSize	Counts packets received that were longer than 1518 octets, or if a VLAN frame 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

| Jabber	The number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
Drop	The number of frames that are dropped by this port since the last Switch reboot.
Time Interval <*1s*>	The time between updates received from the Switch, in seconds. The default is *1s*.
Record Number <*200*>	Select number of times the Switch will be polled between *20* and *200*. The default value is *200.*
Show/Hide	Check whether or not to display CrcError, UnderSize, OverSize, Fragment, Jabber, and Drop errors.

Transmitted Errors
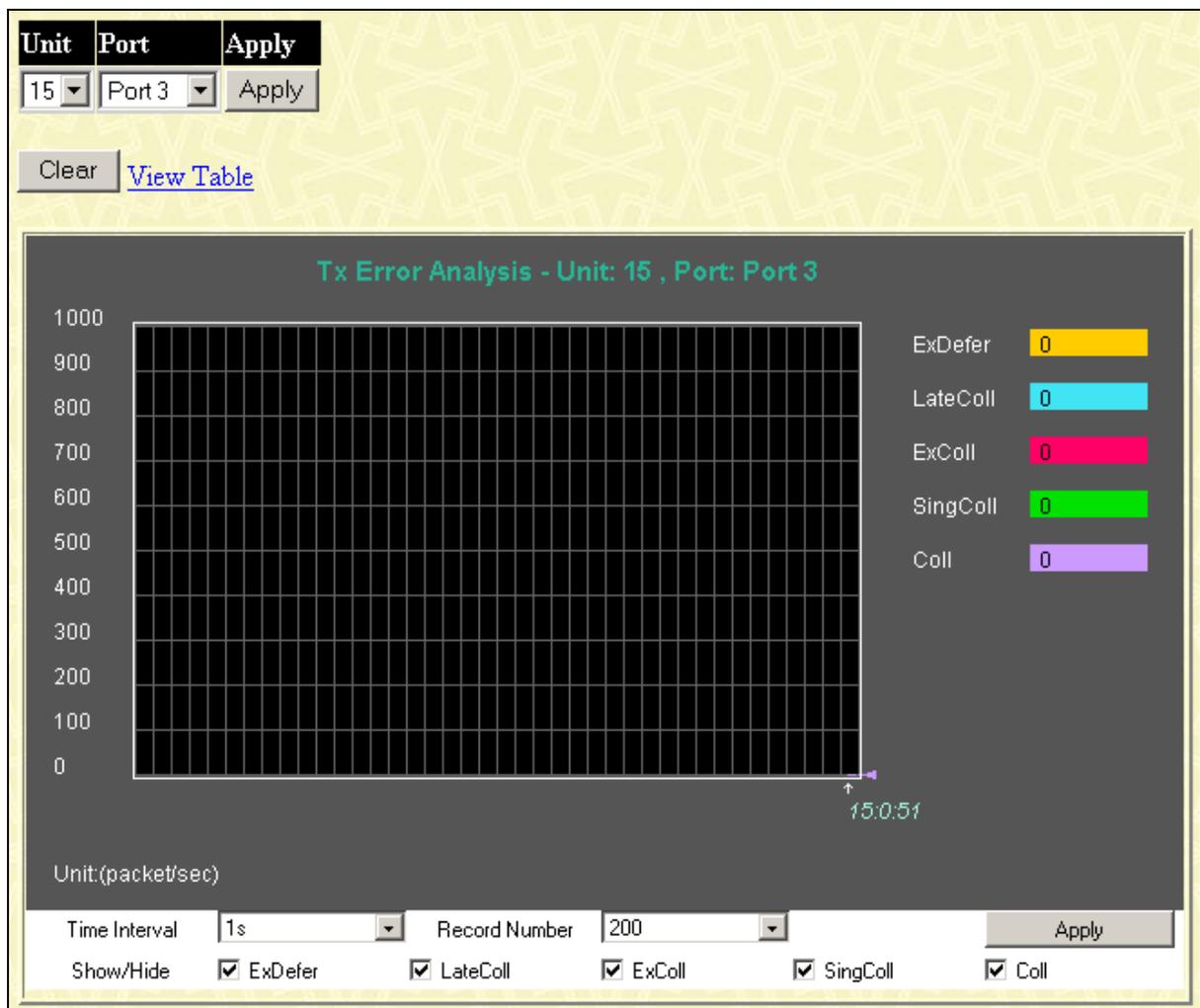
**Figure 7- 13. Tx Error Analysis (line graph) window**
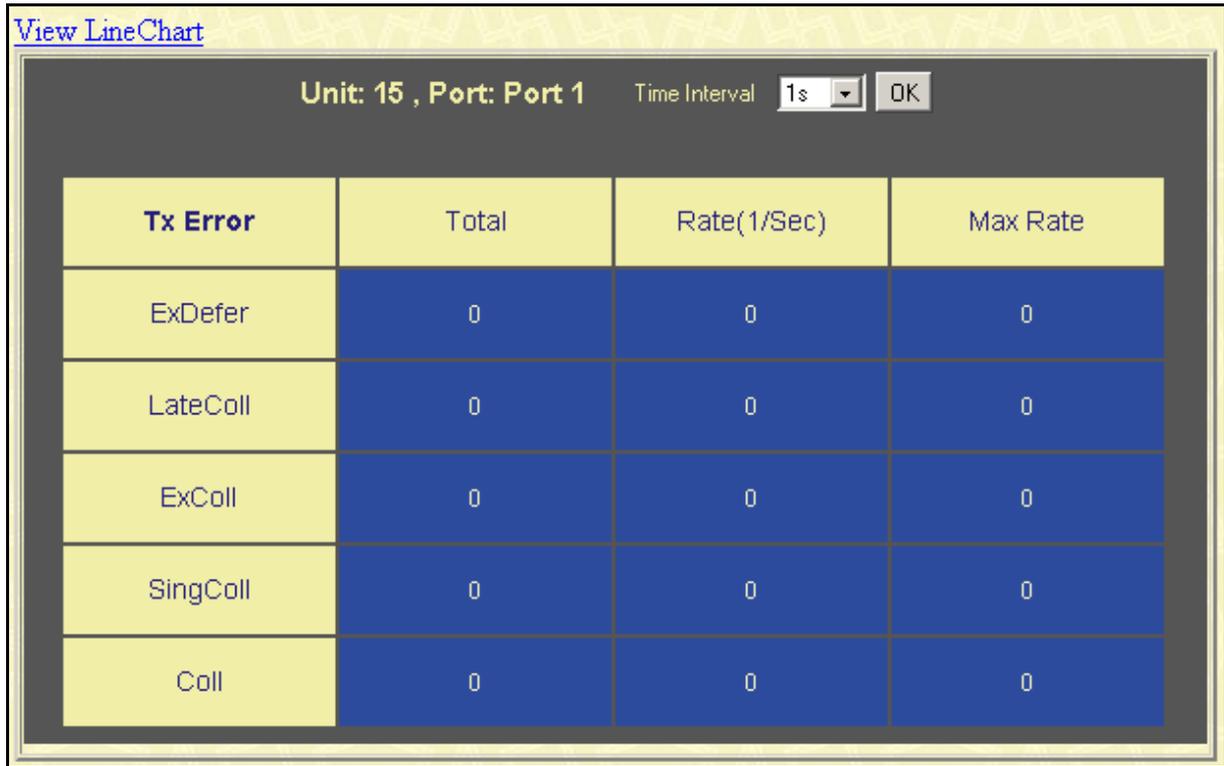
Figure 7- 14. Tx Error Analysis (table) window

Select the desired Switch using the Unit drop-down menu and the desired port using the **Port** drop-down menu. The **Time 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. The number 15 indicates a Switch in standalone mode.
Port	Allows you to specify a port to monitor – from the Switch selected above.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.
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.

115

Time Interval <*1s*>	The time between updates received from the Switch, in seconds. The default is *1s*.
Record Number <*200*>	Select number of times the Switch will be polled between *20* and *200*. The default value is *200.*
Show/Hide	Check whether to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.

Size

Various statistics can be viewed as either a line graph or a table:

- **Packet Size**

Packet Size
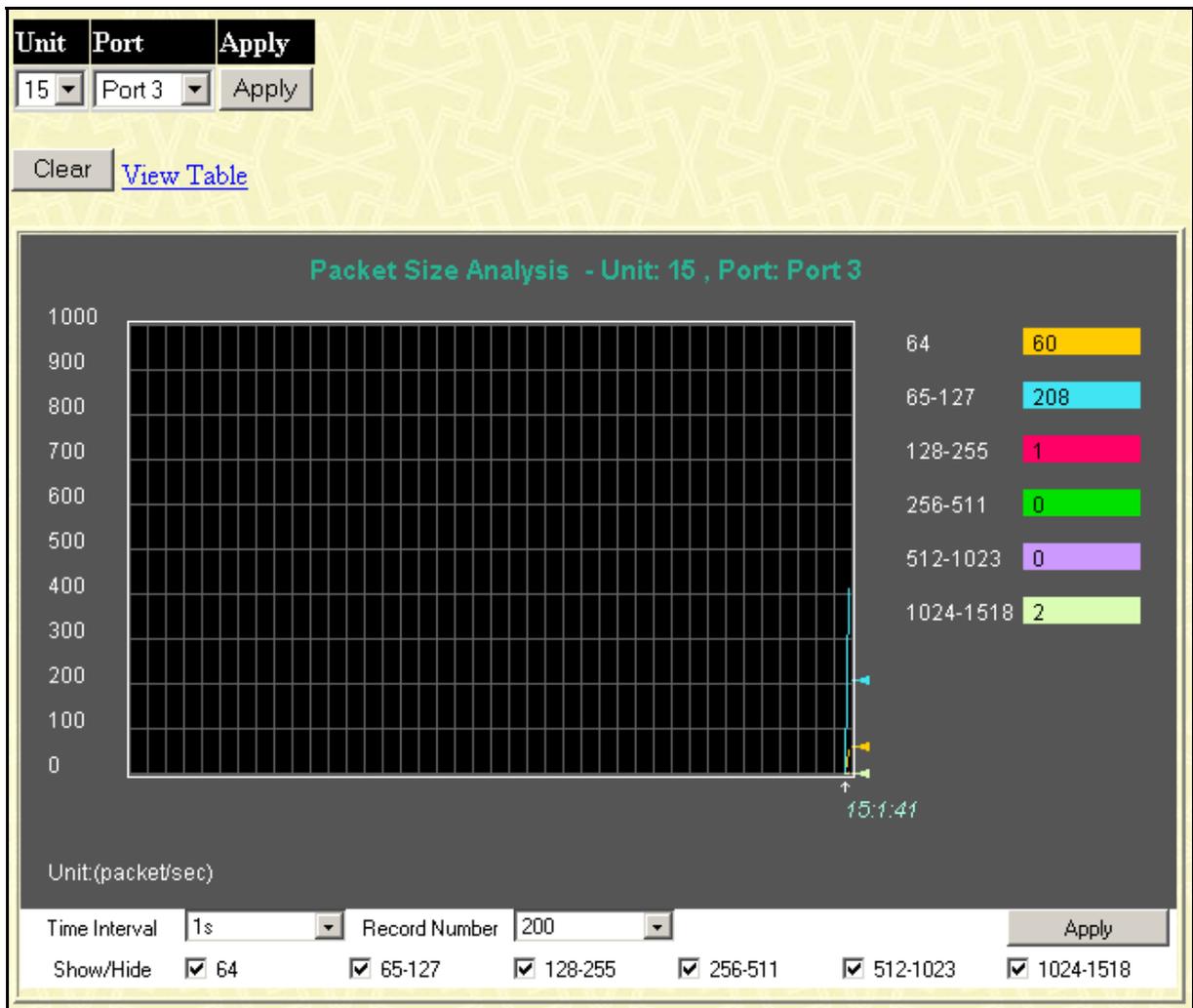
**Figure 7- 15. Packet Size Analysis (line graph) window**
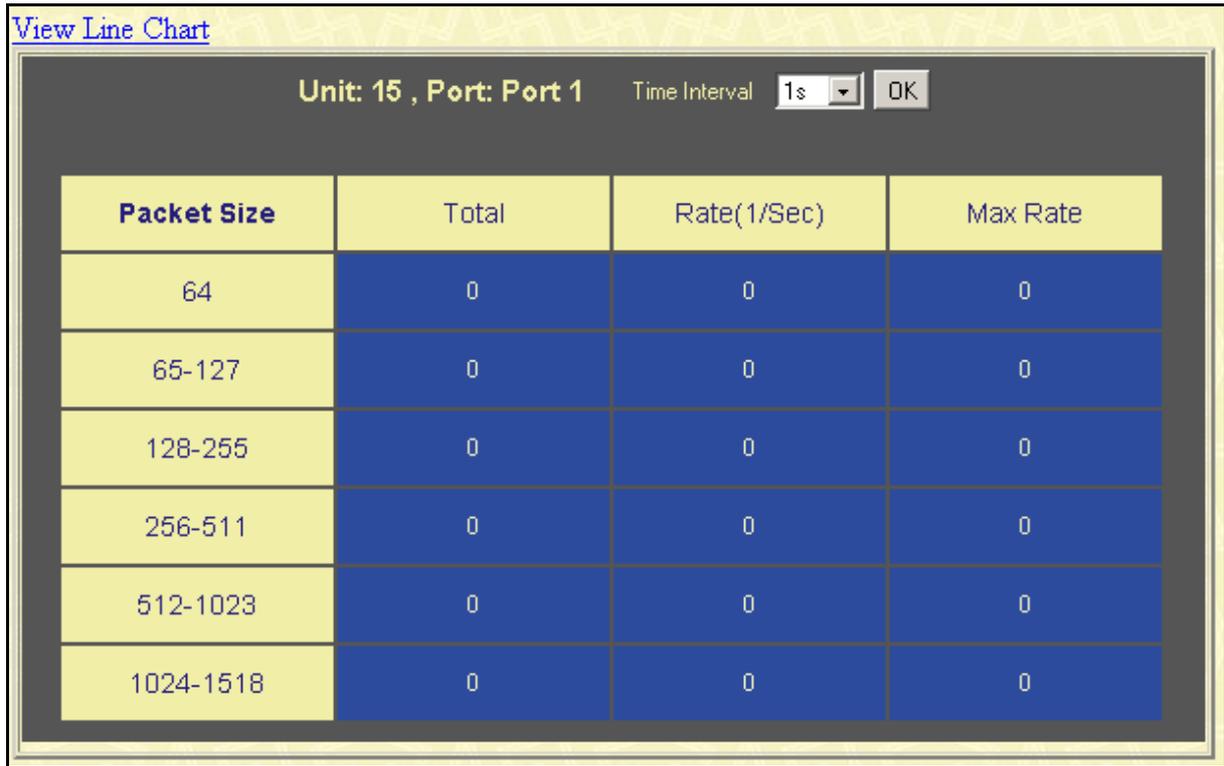
Figure 7- 16. Packet Size Analysis (table) window

Select the desired Switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Time 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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but

	between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Time Interval <*1s*>	The time between updates received from the Switch, in seconds. The default is *1s*.
Record Number <*200*>	Select number of times the Switch will be polled between *20* and *200*. The default value is *200.*
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.

MAC Address

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

Figure 7- 17. MAC Address Table window

The following fields can be set:

Parameter	Description
VLAN ID	Allows you to enter a VLAN ID.
MAC Address	Allows you to specify a MAC Address.
Unit - Port	Enter the desired switch unit and port number.

Switch History

The **Switch History** window displays the Switch's history log, as compiled by the Switch's management agent.

Figure 7- 18. Switch History window

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

The information is described as follows:

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

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.

Figure 7- 19. IGMP Snooping Table window

The following field 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.

Browser 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 7- 20. Browse Router Port window

VLAN Status

This window displays the status of VLANs on any Switch in a Switch stack managed by a DGS-3212SR.

Figure 7- 21. VLAN Status window

Session Table

This window displays the management sessions since the Switch was last rebooted.

Figure 7- 22. Current Session Table window

Authenticator State

The **Authenticator Status** window is found in the **Monitoring** folder. This window allows you to view the setting/status of the Auth PAE State, Backend_State, and Port Status.
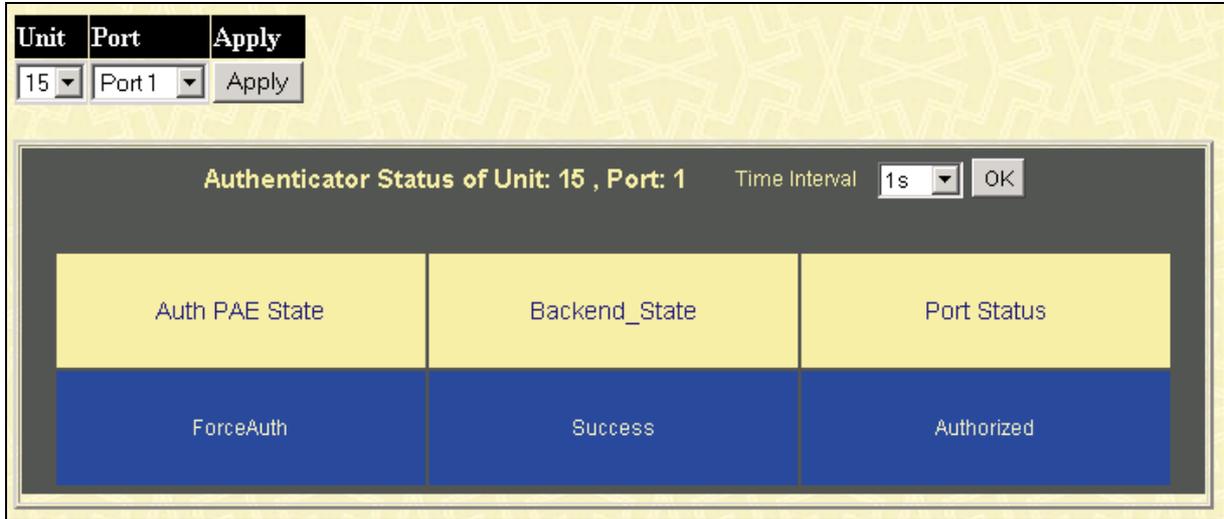
Figure 7- 23. Authenticator Status window

Chapter 8

Maintenance

> ***TFTP Services***
> ***Download Firmware***
> ***Download Configuration File***
> ***Save Settings***
> ***Save History Log***
> ***PING Test***
> ***Save Changes***
> ***Factory Reset***
> ***Restart System***
> ***Logout***

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 8- 1. Download Firmware window

Use the Unit ID drop-down menu to 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. The number 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 8- 2. Use Configuration File on Server window

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

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

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

Save Settings

To upload the Switch settings to a TFTP server, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Save Settings** link:
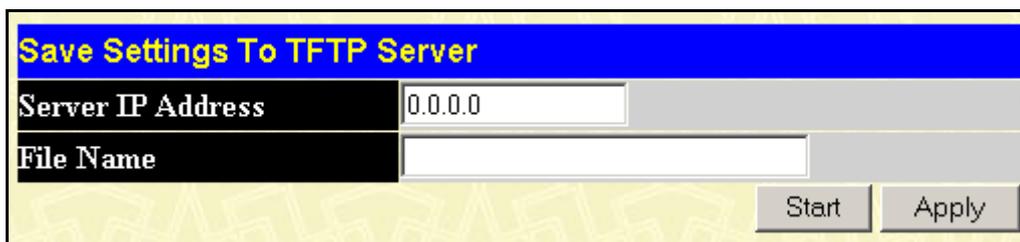
Figure 8- 3. Save Settings To TFTP Server window

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

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

Save History 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 **Save History Log** link:

Figure 8- 4. Save Switch History To TFTP Server window

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

Click **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.
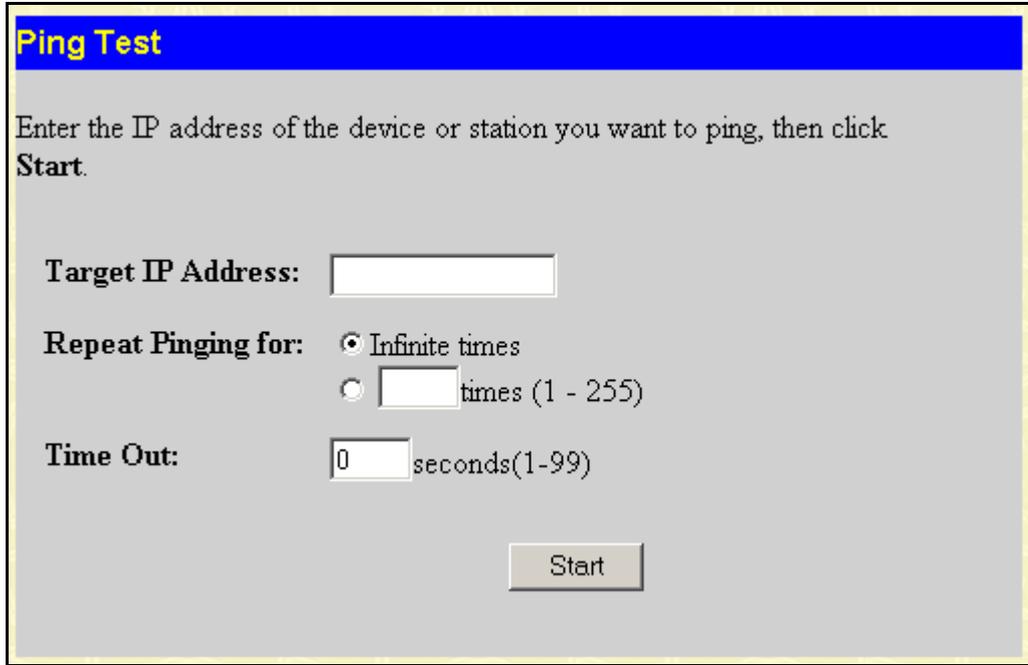
Figure 8- 5. Ping Test window

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-3212SR 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 the **Save Configuration** button in window below.
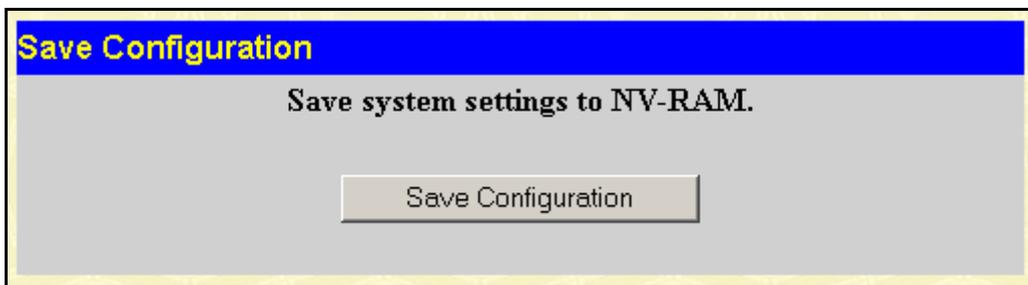
Figure 8- 6. Save Configuration window

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.

Please note that 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.
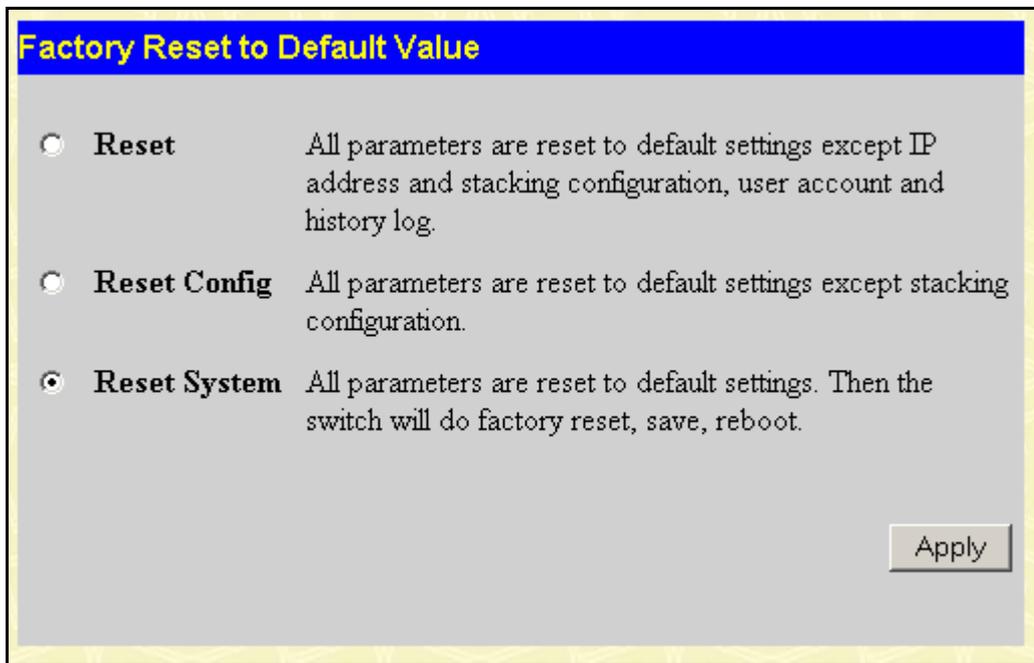
Figure 8- 7. Factory Reset to Default Value window

Restart System

The following window is used to restart the Switch.

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.
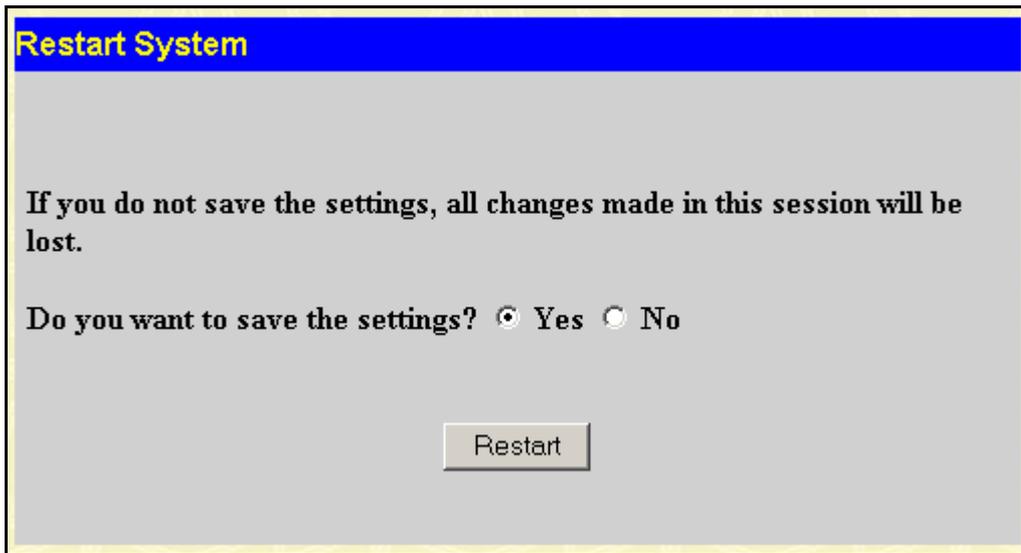
Figure 8- 8. Restart System window

Logout

Use this window to logout of the Switch's Web-based management agent by clicking on the **Log Out** button.
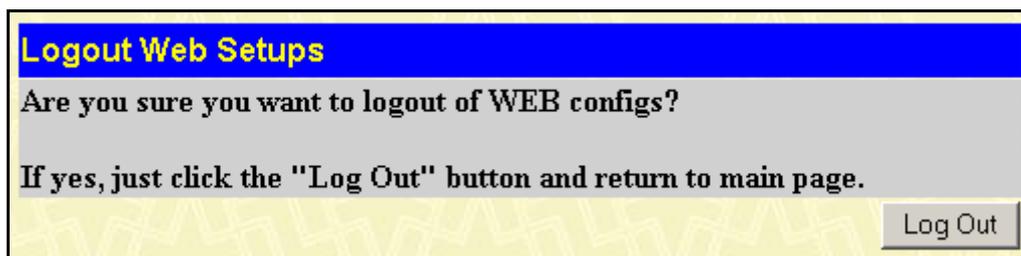
Figure 8- 9. Logout Web Setups window

<div style="border: 1px solid black; display: inline-block; float: right;">

Chapter 9

</div>

Single IP Management

SIM Settings
Topology
Firmware Upgrade
Configuration Backup/Restore

Simply put, Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages to implement "Single IP Management" feature:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.

2. SIM can reduce the number of IP address needed in your network.

3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using Single IP Management (labeled here as SIM) must conform to the following rules:

→ SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.

→ There are three classifications for switches using SIM. The Commander Switch (CS), which is the master switch of the group, Member Switch (MS), which is a switch that is recognized by the CS a member of a SIM group, and a Candidate Switch (CaS), which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

→ A SIM group can only have one Commander Switch (CS).

→ All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

→ A SIM group accepts up to 32 switches (numbered 0-31), including the Commander Switch (numbered 0).

→ There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

→ If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

→ SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that is more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DGS-3212SR may take on three different roles:

→ **Commander Switch (CS)** – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

It has an IP Address.

It is not a command switch or member switch of another Single IP group.

It is connected to the member switches through its management VLAN.

→ **Member Switch (MS)** – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

It is not a CS or MS of another IP group.

It is connected to the CS through the CS management VLAN.

$\rightarrow$ **Candidate Switch (CaS)** – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the DGS-3212SR, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

$\rightarrow$ Each device begins in a Commander state.

$\rightarrow$ CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.

$\rightarrow$ The user can manually configure a CS to become a CaS.

A MS can become a CaS by:

$\rightarrow$ Being configured as a CaS through the CS.

$\rightarrow$ If report packets from the CS to the MS time-out.

$\rightarrow$ The user can manually configure a CaS to become a CS

$\rightarrow$ The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DGS-3212SR switches may join the group either by an automatic method or by manually configuring the switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

All DGS-3212SR switches are set as Candidate (CaS) switches, as their factory default configuration and the Single IP Management feature will be disabled. To enable SIM for the Switch using the Web interface, go to the **Single IP Management** folder and click the **SIM Settings** link, revealing the following window.

SIM Settings

Figure 9- 1. SIM Settings window (SIM State *Disabled*)

Change the SIM State to *Enabled* using the pull-down menu and click **Apply**. The window will then refresh and the **SIM Settings** window will look like this:

Figure 9- 2. 2nd SIM Settings window (SIM State *Enabled*)

The following parameters can be set:

Parameters	Description
SIM State	Use the pull-own menu to either enable or disable the SIM state on the Switch. *Disabled* will render all SIM functions on the Switch inoperable.
Role State	Use the pull-down menu to change the SIM role of the Switch. The two choices are: *Candidate* – A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the DGS-3212SR. *Commander* – Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Discovery Interval	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from *30* to *90* seconds.
Holdtime	This parameter may be set for the time, in seconds that the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from *100* to *255* seconds.

Click **Apply** to implement the settings changed.

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain three added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade** and **Configuration Backup/Restore**.

Topology

The topology windows will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer. The following message should appear the first time the user clicks the **Topology** link in the **Single IP Management** folder.

Figure 9- 3. Java window

Clicking the here link will setup the Java Runtime Environment on your server and lead you to the opening topology window, as seen below.

Figure 9- 4. Tree View window

The Tree View window holds the following information under the **Data** tab:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Speed	Displays the connection speed between the CS and the MS or CaS.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.

MAC Address	Displays the MAC Address of the corresponding Switch.
Model Name	Displays the full Model Name of the corresponding Switch.

To view the Topology Map, click the **View** menu in the toolbar and then select **Topology**, which will produce the following window. The **Topology View** window will refresh itself periodically (20 seconds by default).
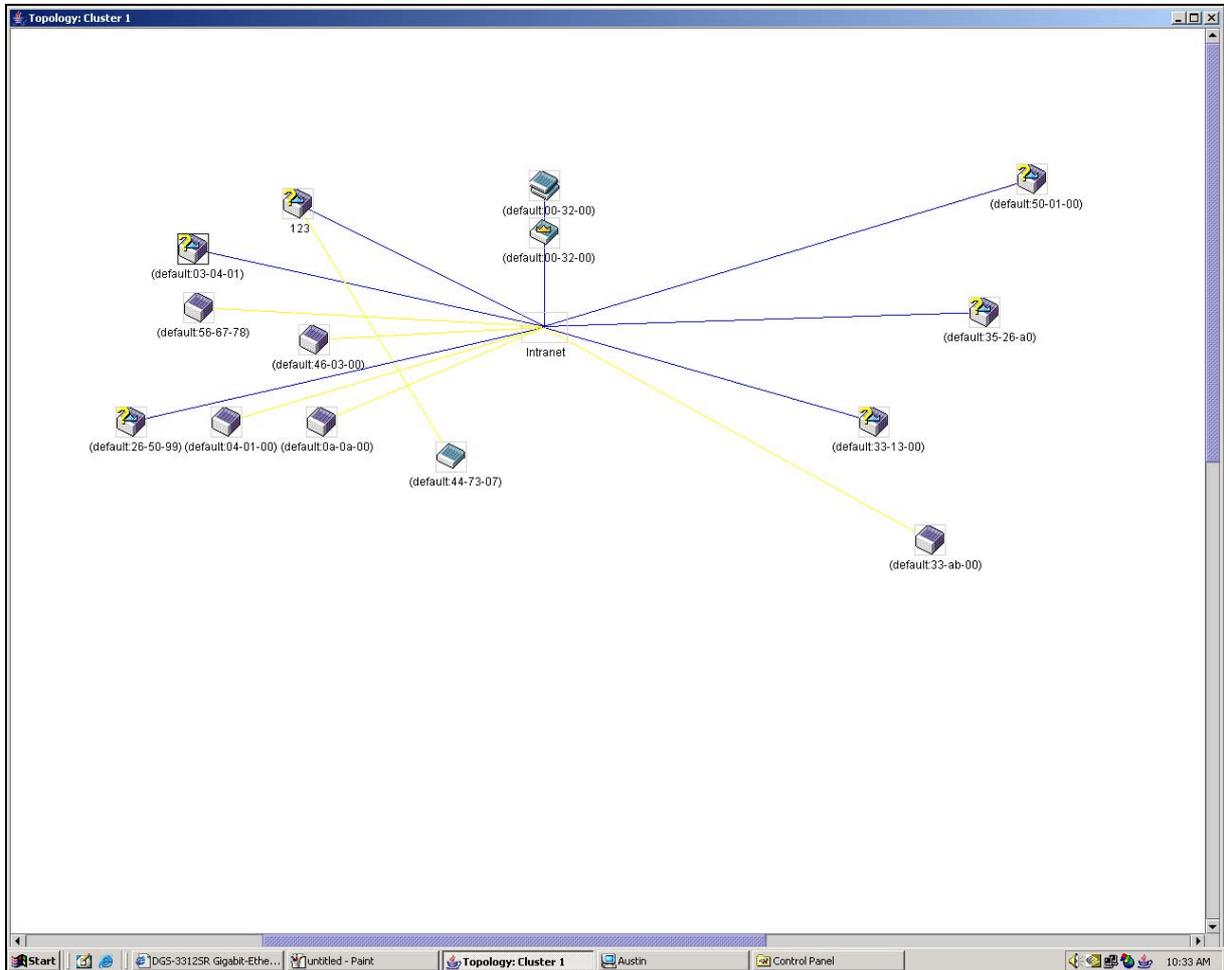
Figure 9- 5. Topology View window

This window will display how the devices within the Single IP Management Group are connected to other groups and devices. Possible icons in this window are as follows:

Icon	Description
	Group
	Layer 2 commander switch
	Layer 3 commander switch
	Commander switch of other group

	Layer 2 member switch.
	Layer 3 member switch
	Member switch of other group
	Layer 2 candidate switch
	Layer 3 candidate switch
	Unknown device
	Non-SIM devices

Tool Tips

In the **Topology View** window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree View does. See the window below for an example.
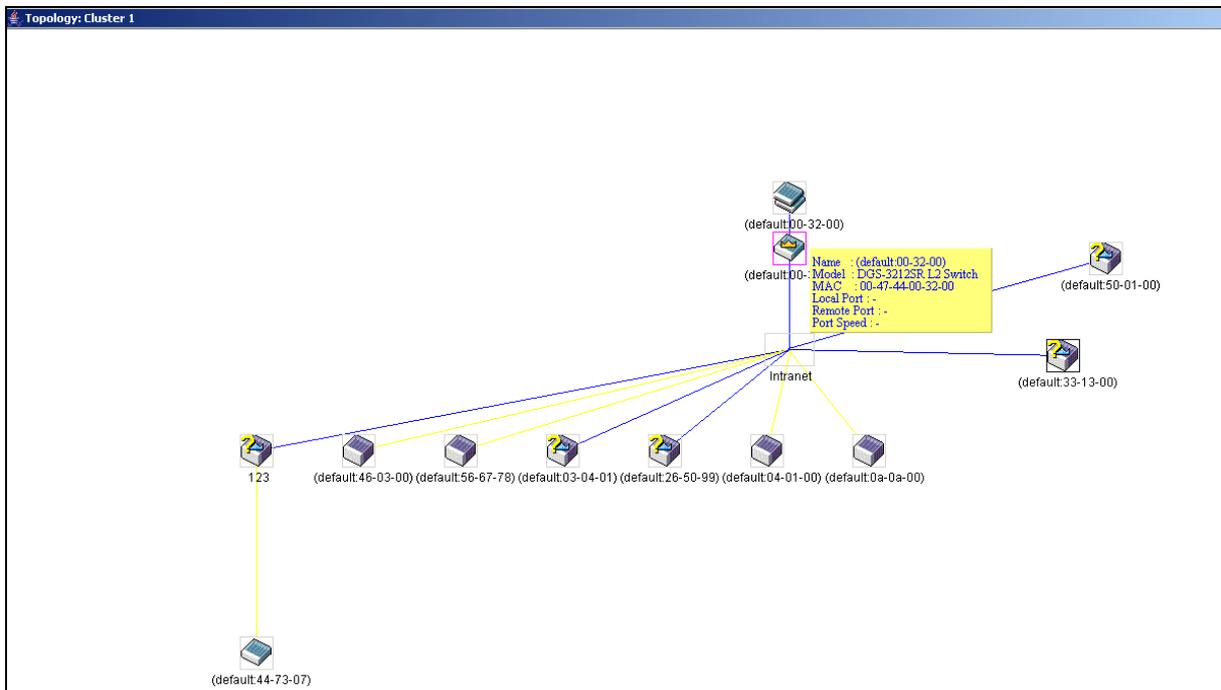
Figure 9- 6. Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between two devices, as shown below.
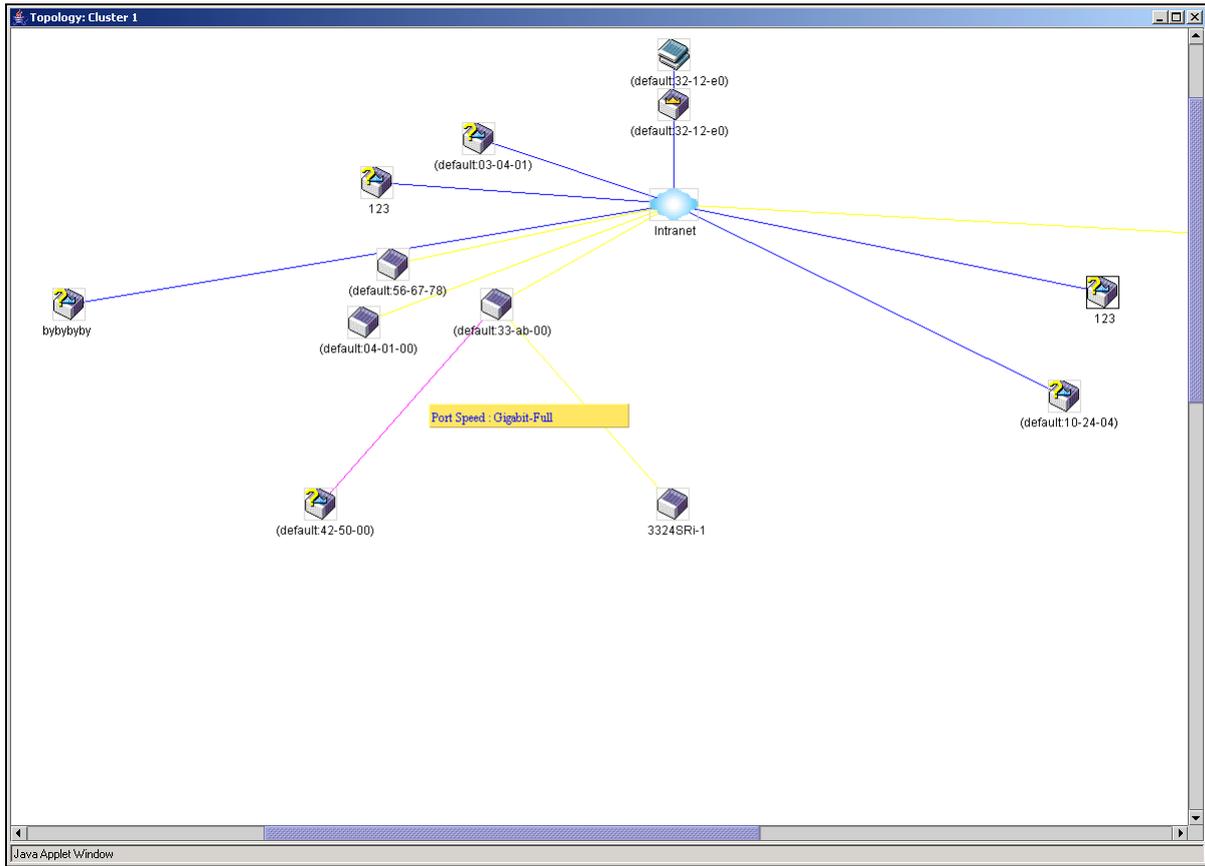
Figure 9- 7. Port Speed Utilizing the Tool Tip

Right-click

Right-clicking on a device will allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group Icon
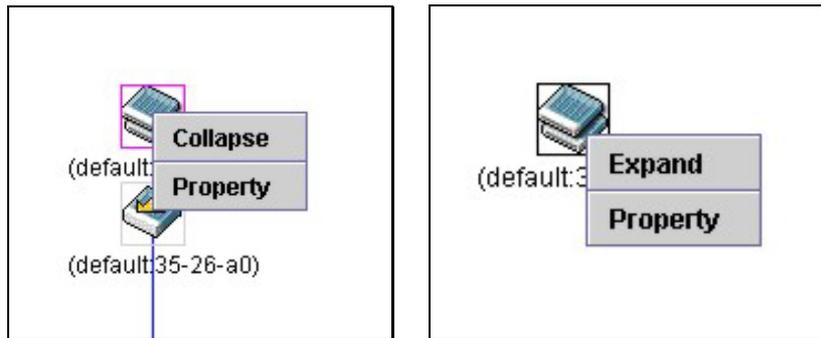
Figure 9- 8. Right-clicking a Group icon

The following options may appear for the user to configure:

Collapse - To collapse the group that will be represented by a single icon.

Expand - To expand the group in detail. CS, MS and CaS in this group are shown.

Property - To pop up a window to display the group information.

Commander Switch Icon
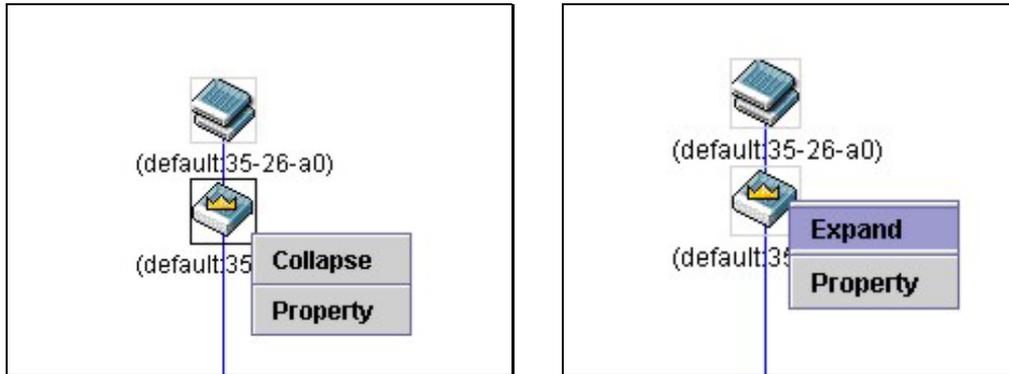
Figure 9- 9. Right-clicking a Commander icon

The following options may appear for the user to configure:

Collapse - To collapse the group that will be represented by a single icon.

Expand - To expand the group in detail. CS, MS and CaS in this group are shown.

Property - To pop up a window to display the group information.

Member Switch Icon
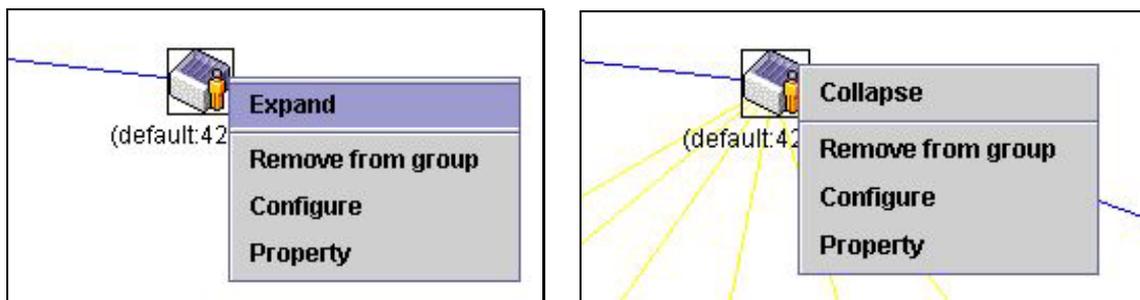
Figure 9- 10. Right-clicking a Member icon

The following options may appear for the user to configure:

Collapse - To collapse the group that will be represented by a single icon.

Expand - To expand the group in detail. CS, MS and CaS in this group are shown.

Remove from group - Remove a member from a group.

Configure - Launch the web management to configure the switch.

Property - To pop up a window to display the device information.

Candidate Switch Icon
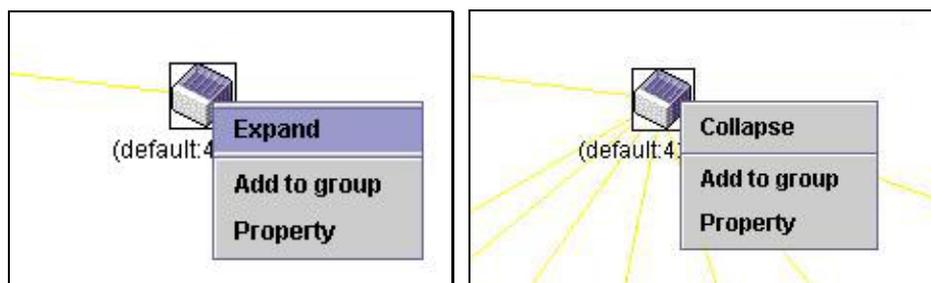
Figure 9- 11. Right-clicking a Candidate icon

137

The following options may appear for the user to configure:

Collapse - To collapse the group that will be represented by a single icon.

Expand - To expand the group in detail. CS, MS and CaS in this group are shown.

Add to group - Add a candidate to a group.

Property - To pop up a window to display the device information, as shown below.
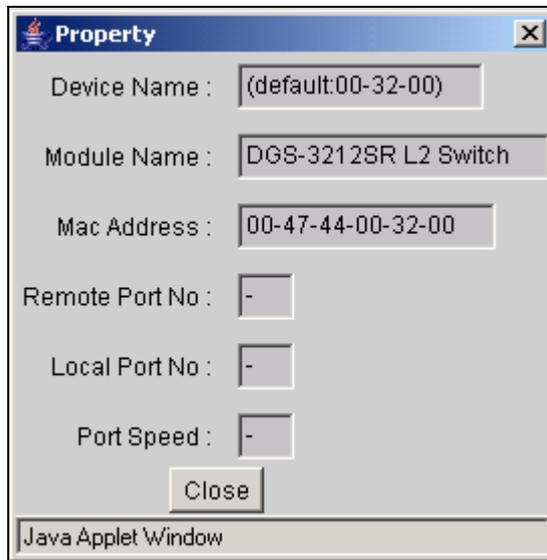
Figure 9- 12. Property window

Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.

Figure 9- 13. Topology View menu bar

The five menus on the menu bar are as follows.

File

Print Setup - Will view the image to be printed.

Print Topology- Will print the topology map.

Preference - Will set display properties, such as polling interval, and the views to open at SIM startup.
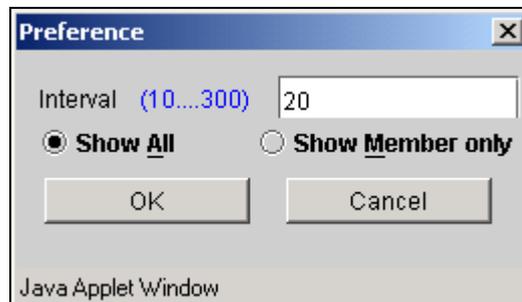
Figure 9- 14. Preference dialog box

Group

Add to Group - Add a CaS to the group.

Remove from Group - Remove an MS from the group.

Device

Configure – Will open the web manager for the specific device.

View

Refresh - Update the views with the latest status.

Topology - Display the Topology view.

Help

About – Will display the SIM information, including the version number.

Figure 9- 15. About dialog box

> **NOTE:** Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the ***DGS-3212SR Command Line Interface Reference Manual*** for more information on SIM and its configurations.

Firmware Upgrade

This window is used to upgrade firmware from the commander switch to the member switch. Member switches will be listed in the table and will be specified by Port (port on the CS where the MS resides), MAC Address, Model Name and Version. To specify a certain Switch for firmware download, click its corresponding check box under the Port heading. To update the firmware, enter the Server IP Address where the firmware resides and enter the Path/Filename of the firmware. Click **Download** to initiate the file transfer.
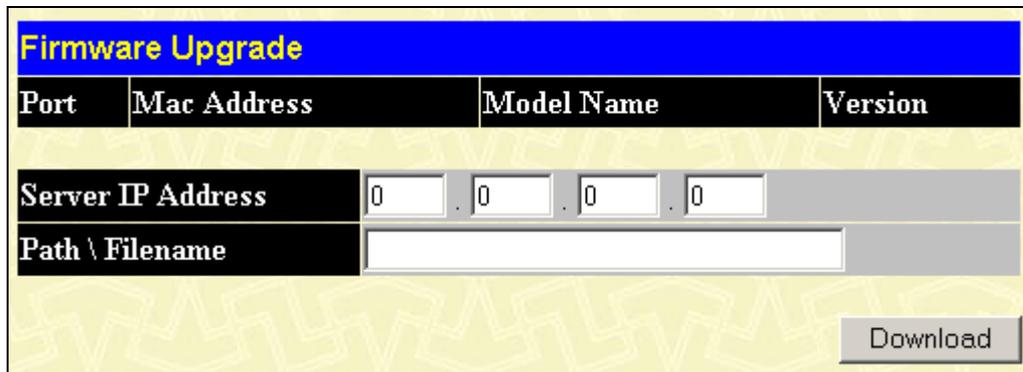
Figure 9- 16. Firmware Upgrade window

Configuration File Backup/Restore

This window is used to upgrade configuration files from the commander switch to the member switch. Member switches will be listed in the table and will be specified by Port (port on the CS where the MS resides), MAC Address, Model Name and Version. To specify a certain Switch for upgrading configuration files, click its corresponding radio button under the Port heading. To update the configuration file, enter the Server IP Address where the firmware resides and enter the Path/Filename of the firmware. Click **Download** to initiate the file transfer.

Figure 9- 17. Configuration File Backup/Restore window

Appendix A

Technical Specifications

General	
Standard	IEEE 802.3 10BASE-T Ethernet
	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:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	N/A 2000Mbps
Fiber Optic	IEC 793-2:1992
	Type A1a - 50/125um multimode
	Type A1b - 62.5/125um multimode
	Both types use LC optical connector
Topology	Star
Network Cables	UTP Cat. 5 for 100Mbps
	UTP Cat. 3, 4, 5 for 10Mbps
	EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	1 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.

Physical & Environmental	
AC inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	30 watts maximum
DC fans:	1 built-in 75 x 75 x30 mm fan
Operating Temperature:	0 to 40 degrees Celsius (32 to 104 degrees Fahrenheit)
Storage Temperature:	-25 to 55 degrees Celsius (-13 to 131 degrees Fahrenheit)
Humidity:	Operating: 5% to 95% RH, non-condensing Storage: 0% to 95% RH, non-condensing
Dimensions:	441 mm x 309 mm x 44 mm (17.36 x 12.16 x 1.73 inches), 1UHeight, 19 inch rack-mount width
Weight:	4.4 kg (9.7 lbs.)
EMI:	FCC Class A, CE Mark, C-Tick
Safety:	CSA International

Glossary

100BASE-FX: 100Mbp 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.

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

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

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

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: A configurable designation for RSTP operations. It defines a port that is directly connected to a segment where a loop cannot exist. For example, a port connected to a server with a single Ethernet connection. Edge ports transition to a forwarding state more quickly where RSTP is used.

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.

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

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

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

RSTP: Rapid Spanning Tree Protocol as defined by IEEE 802.1w.

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

SLIP: Serial Line Internet Protocol. A protocol that 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. The IEEE standard 802.1d describes how the protocol.

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

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.

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

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.

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address/telephone/fax/e-mail/Web site list of D-Link offices is provided in the back of this manual.

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

D-Link or its authorized reseller or distributor and

Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

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

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

Hardware for as long as the original customer/end user owns the product, or five years after product discontinuance, whichever occurs first (excluding power supplies and fans)

Power Supplies and Fans Three (3) Year

Spare parts and spare kits Ninety (90) days

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

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

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

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

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

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

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

The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc, 17595 Mt. Herrmann, Fountain Valley, CA 92708-4160, USA. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

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

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

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

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

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

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

Copyright Statement: No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright© 2003 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

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

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

Trademarks

Copyright ©2004 D-Link Corporation.
Contents subject to change without prior notice.
D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976.

FCC Warning

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

CE Mark Warning

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

D-Link Offices

Australia	**D-Link Australasia** 1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia TEL: 61-2-8899-1800 FAX: 61-2-8899-1868 URL: www.dlink.com.au
Belgium	**D-Link Belgium** Rue des Colonies 11, B-1000 Brussels, Belgium TEL: 32 (0)2 517 7111 FAX: 32 (0)2 517 6500 URL: www.dlink-benelux.com
Brazil	**D-Link Brasil Ltda.** Av das Naçōes Unidas, 11857, cj 132 – Brooklin Novo, São Paulo, Brasil 04578-000 TEL: (55 11) 5503-9320 FAX: (55 11) 5503-9321 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 URL: www.dlink.ca
Chile	**D-Link South America (Sudamérica)** Isidora Goyenechea 2934 Oficina 702 Las Condes Fono 2323185, Santiago, Chile TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: www.dlink.cl
China	**D-Link China** Room 507/508, Tower W1, The Towers, Oriental Plaza No. 1 East Chang An Ave., Dong Cheng District, Beijing, 100738, China TEL: (86-010) 85182533 FAX: (86-010) 85182250 URL: www.dlink.com.cn
Denmark	**D-Link Denmark** Naverland 2, DK-2600 Glostrup, Denmark TEL: 45-43-96-90-40 FAX: 45-43-42-43-47 URL: www.dlink.dk
Egypt	**D-Link Egypt** 19 El-Shahed Helmy, El Masry, Al-Maza, Heliopolis, Cairo, Egypt TEL: 202-41-44-295 FAX: 202-41-56-704 URL: www.dlink-me.com
Finland	**D-Link Finland** Pakkalankuja 7A, 3rd floor, 01510 Vantaa, Finland TEL: 358-9-2707-5080 FAX: 358-9-2707-5081 URL: www.dlink.fi
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
Germany	**D-Link Central Europe (D-Link Deutschland GmbH)** Schwalbacher Strasse 74, D-65760 Eschborn, Germany TEL: 49-6196-77990 FAX: 49-6196-7799300 URL: www.dlink.de
India	**D-Link India** D-Link House, Kurla-Bandra Complex Rd., Off Cst Rd., Santacruz (East), Mumbai, 400 098 India TEL: 91-022-652-6696/6578/6623 FAX: 91-022-652-8914/8476 URL: www.dlink.co.in & www.dlink-india.com

Israel	**D-Link Israel**
	11 Hamanofim Street, Ackerstein Towers, Regus Business Center
	P.O.B. 2148, Hertzelia-Pituach 46120, Israel
	TEL: 972-9-9715700 FAX: 972-9-9715601
	URL: www.dlink.co.il
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
Netherlands	**D-Link Netherlands**
	Weena 290, 3012 NJ Rotterdam, The Netherlands
	TEL: 31 (0)10 282 1445 FAX: 31 (0)10 282 1331
	URL: www.dlink-benelux.com
Norway	**D-Link Norway**
	Karihaugveien 89, N-1086 Oslo
	TEL: 47-23-89-71-89 FAX: 47-22-30-90-85
	URL: www.dlink.no
Russia	**D-Link Russia**
	Grafsky per., 14, floor 6, Moscow 129626 Russia
	TEL: 7 (095) 744-0099 FAX: 7 (095) 744-0099 #350
	URL: www.dlink.ru
Singapore	**D-Link International**
	1 International Business Park, #03-12 The Synergy, Singapore 609917
	TEL: 65-6774-6233 FAX: 65-6774-6322
	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
Spain	**D-Link Iberia**
	C/Sabino de Arana, 56 Bajos, 08028 Barcelona, Spain
	TEL: 34 93 409 0770 FAX: 34 93 491 0795
	URL: www.dlink.es
Sweden	**D-Link Sweden**
	P. O. Box 15036, S-167 15 Bromma, Sweden
	TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901
	URL: www.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
Turkey	**D-Link Turkey**
	Regus Offices Beybi Giz Plaza, Ayazaga Mah. Meydan Sok. No. 28
	Maslak 34396, Istanbul-Turkiye
	TEL: 90-212-335-2553 FAX: 90-212-335-2500
	URL: www.dlink.com.tr
U.A.E.	**D-Link Middle East**
	P.O. Box 500376, Office No. 103, Building 3
	Dubai Internet City, Dubai, United Arab Emirates
	TEL: 971-4-3916480 FAX: 971-4-3908881
	URL: www.dlink-me.com
U.K.	**D-Link Europe (United Kingdom)**
	4th Floor, Merit House, Edgware Road, Colindale, London
	NW9 5AB United Kingdom
	TEL: 44-020-8731-5555 FAX: 44-020-8731-5511
	URL: www.dlink.co.uk

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____

Organization: _____Dept._____

Your title at organization:_____ Telephone:_____ Fax:_____

Organization's full address:_____

Country:_____

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

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

(* Applies to adapters only)

Product was purchased from:

Reseller's name:_____

Telephone:_____ Fax:_____

Reseller's full address:_____

_____

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

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

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

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

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

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

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

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

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

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

10.Your comments on this product?

_____
_____
_____
_____
_____
_____

TO:

D-Link®