D-Link®

# DGS-3208TG
# Gigabit Ethernet Switch
# User’s Guide

First Edition (July 2000)
6DGS3208TG01
Printed In Taiwan

RECYCLABLE

# Wichtige Sicherheitshinweise

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

1. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

## WARRANTIES EXCLUSIVE

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

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

## LIMITATION OF LIABILITY

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

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

# Limited Warranty

## Hardware:

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

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

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

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

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

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

## Software:

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

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

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

## 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.

## Trademarks

## Copyright Statement

## 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.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### CE Mark Warning:

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

### Warnung!

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

### Precaución!

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

### Attention!

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

### Attenzione!

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

## VCCI Warning

### 注意

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## BSMI Warning

### 警告使用者

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

# TABLE OF CONTENTS

# ABOUT THIS GUIDE

This user's guide tells you how to install your DGS-3208TG stand-alone Switch, how to connect it to your Gigabit Ethernet network, and how to set its configuration using either the built-in console interface or Web-based management.

## Terms

For simplicity, this documentation uses the terms "Switch" (first letter upper case) to refer to the DGS-3208TG Gigabit Ethernet Switch, and "switch" (first letter lower case) to refer to all Ethernet switches, including the DGS-3208TG.

## Overview of this User's Guide

- Chapter 1, "*Introduction*." Describes the Switch and its features.
- Chapter 2, "*Unpacking and Setup*." Helps you get started with the basic installation of the Switch.
- Chapter 3, "*Identifying External Components*." Describes the front panel, rear panel, side panels, and LED indicators of the Switch.
- Chapter 4, "*Connecting the Switch*." Tells how you can connect the DGS-3208TG to your Gigabit Ethernet network.
- Chapter 5, "*Switch Management Concepts*." Talks about local console management via the RS-232 DCE console port and other aspects about how to manage the Switch.
- Chapter 6, "*Using the Console Interface*." Tells how to use the built-in console interface to change, set, and monitor Switch performance and security.
- Chapter 7, "*Web-Based Network Management*." Tells how to manage the Switch through an Internet browser.
- Appendix A, "*Technical Specifications*." Lists the technical specifications of the DGS-3208TG.

# 1

# INTRODUCTION

This section describes the features of the DGS-3208TG, as well as giving some background information about Gigabit Ethernet and switching technology.

## Gigabit Ethernet Technology

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

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

Gigabit Ethernet enables fast fiber-optic and copper connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. And with expected advances in the coming years in silicon technology and digital signal processing that will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, outfitting your network with a powerful 1000-Mbps-capable backbone/server connection creates a flexible foundation for the next generation of network technology products.

## Switching Technology

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

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by making it possible for a local area network to be divided into different *segments* which don't compete with each other for network transmission capacity, giving a decreased load on each.

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

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

# Features

The DGS-3208TG Gigabit Ethernet Switch was designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continuously.

Switch features include:

## *Ports*

- Six 100BASE-TX/1000BASE-T (Fast Ethernet/Gigabit Ethernet) ports with cable-ready RJ-45 jacks.
- Two GBIC (Gigabit Interface Converter) slots, able to accommodate GBICs for all standard Gigabit Ethernet cabling.
- RS-232 DCE console port for diagnosing the Switch via a connection to a PC and console/out-of-band management.

## *Performance features*

- Store and forward switching scheme capability to support rate adaptation and protocol conversion.
- Full duplex to allow two communicating stations to transmit and receive at the same time.
- Data forwarding rate 1,488,100 pps per port at 100% of wire-speed for 1000-Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 1,488,100 pps per port at 100% of wire-speed for 1000-Mbps speed.
- 12K active MAC address entry table per device with automatic learning and aging.
- 16 MB packet buffer per device.
- Supports broadcast storm rate filtering.
- Supports IGMP snooping.
- Supports port mirroring.
- Supports GVRP.
- Supports GMRP (802.1P).
- Supports 802.1P priority (tag mode).
- Supports static filtering (based on MAC Address)

- Supports port-based VLAN (overlapping VLANs are excluded).
- Supports IEEE 802.1Q VLAN.
- Supports Link Aggregation Capability.

## Management

- RS-232 console port for out-of-band management via a PC.
- IEEE 802.1d Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of indefinite network loops.
- Fully configurable either in-band or out-of-band control via SNMP based software.
- Flash memory for software upgrade. This can be done in-band via BOOTP/TFTP. Out-of-band console can also initiate a download request.
- Built-in SNMP management: Bridge MIB (RFC 1493), RMON MIB (RFC 1757), MIB-II (RFC 1213), VLAN MIB (802.1Q), 802.1D MIB, and D-Link proprietary MIB.

# 2

# UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Switch.

## Unpacking

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

- ♦ One DGS-3208TG Gigabit Ethernet Switch
- ♦ Accessory pack: 2 mounting brackets and screws
- ♦ Four rubber feet with adhesive backing
- ♦ One AC power cord
- ♦ One user's guide on CD-ROM with Registration Card

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

## Setup

The setup of the Switch can be performed using the following steps:

- ♦ The surface must support at least 5 kg.
- ♦ The power outlet should be within 1.82 meters (6 feet) of the device.
- ♦ Visually inspect the power cord and see that it is secured fully to the AC power connector.
- ♦ Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Do not place heavy objects on the Switch.

## Desktop or Shelf Installation

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

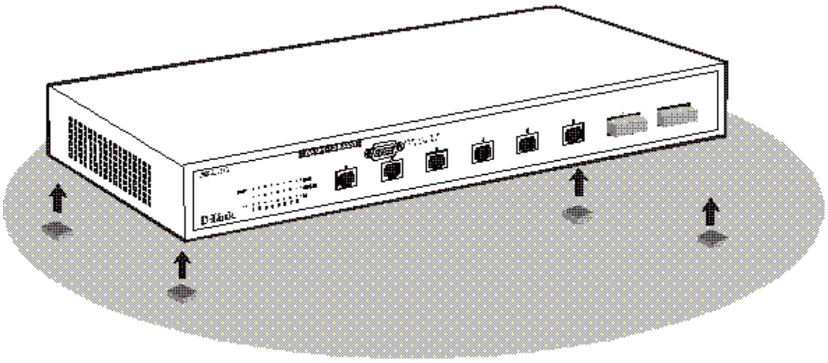


Figure 2-1. Gigabit Ethernet Switch installed on a Desktop or Shelf

# Rack Installation

The DGS-3208TG can be mounted in an EIA standard size, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the switch’s front panel (one on each side) and secure them with the screws provided.

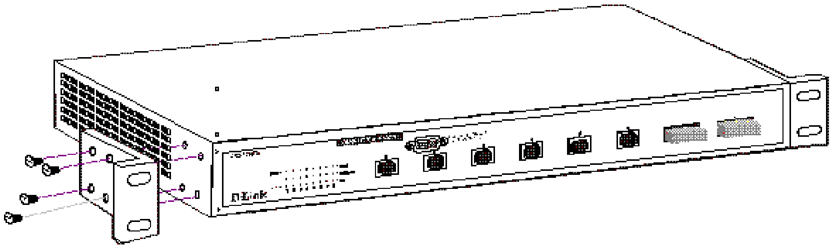


Figure 2- 2A. Attaching the mounting brackets to the Switch

Then, use the screws provided with the equipment rack to mount the Switch in the rack.

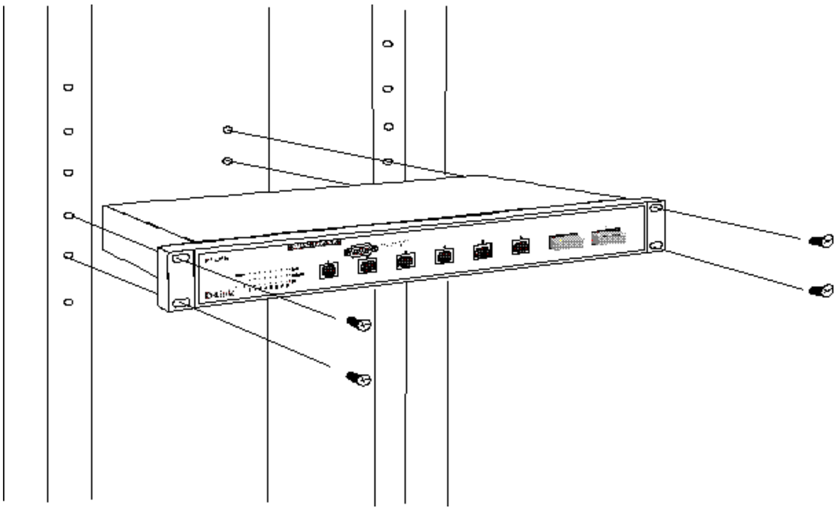


Figure 2-2B. Installing the Switch in an equipment rack

# Power on

The DGS-3208TG Switch can be used with AC power sources 100 - 240 VAC, 50 - 60 Hz. The Switch's power supply will adjust to the local power source automatically and may be turned on without having any or all LAN segment cables connected.

After the device is powered on, the LED indicators should respond as follows:

- The Power LED indicator will light while the Switch loads onboard software, and should remain on as long as the switch has power.

- The Console LED indicator will remain *ON* if there is a connection at the RS-232 port, otherwise this LED indicator is *OFF*.

## *Power Failure*

As a precaution, the Switch should be unplugged in case of power failure. When power is resumed, plug the Switch back in.

3

# IDENTIFYING EXTERNAL COMPONENTS

This chapter describes the front panel, rear panel, side panels, and LED indicators of the Switch

## Front Panel

The front panel of the Switch consists of six 1000BASE-T ports, two GBIC (Gigabit Interface Converter) slots, an RS-232 communication port, and LED indicators.

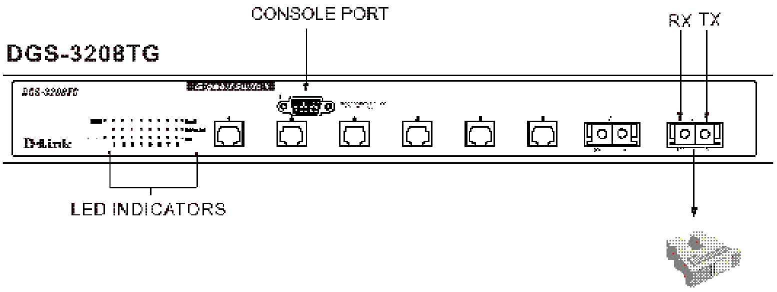


**Figure 3-1. Front panel view of the DGS-3208TG Switch**

- ♦ The six 1000BASE-T ports allow 100/1000-Mbps connections to workstations, servers, and networking devices through four-pair Category 5 twisted-pair cabling.
- ♦ The two GBIC slots accept hot-swappable slide-in modules for 1000BASE-SX multimode optical fiber and other Gigabit Ethernet cable types.
- ♦ An RS-232 DCE console port is for diagnosing the Switch via a connection to a PC and local console management.
- ♦ Comprehensive LED indicators display the condition of the Switch and status of the network. A description of these LED indicators follows (see *LED Indicators*).

## Rear Panel

The rear panel of the Switch consists of an AC power connector. The following shows the rear panel of the Switch.

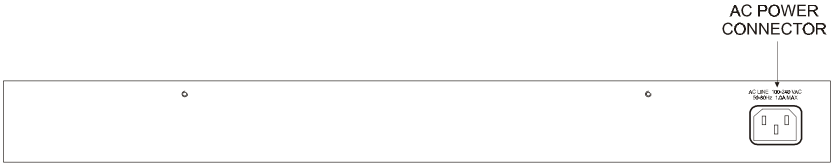


**Figure 3-2. Rear panel view of the DGS-3208TG**

- ♦ **AC Power Connector** This is a three-pronged connector that supports the power cord. Plug in the female connector of the provided power cord into this connector, and the male into a power outlet. Supported input voltages range from 100 ~ 240 VAC at 50 ~ 60 Hz.

# Side Panels

The Switch's side panels contain the system fans, two on the right and one on the left. The following shows the Switch's right side panel.

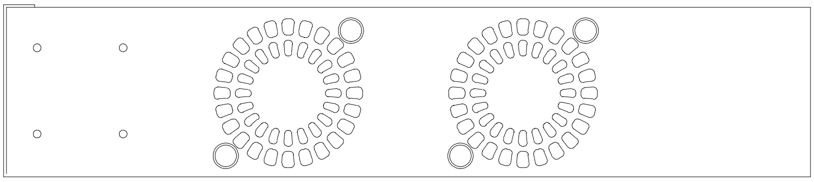


**Figure 3-3. Right side panel view of the DGS-3208TG**

- ♦ **System Fans** These fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Be sure not to block these openings, and to leave adequate space at the rear and sides of the Switch for proper ventilation. Remember that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

# LED Indicators

The LED indicators of the Switch include Power, Console, Speed, Link/ACT, and Full. The following shows the LED indicators for the Switch along with an explanation of each indicator.

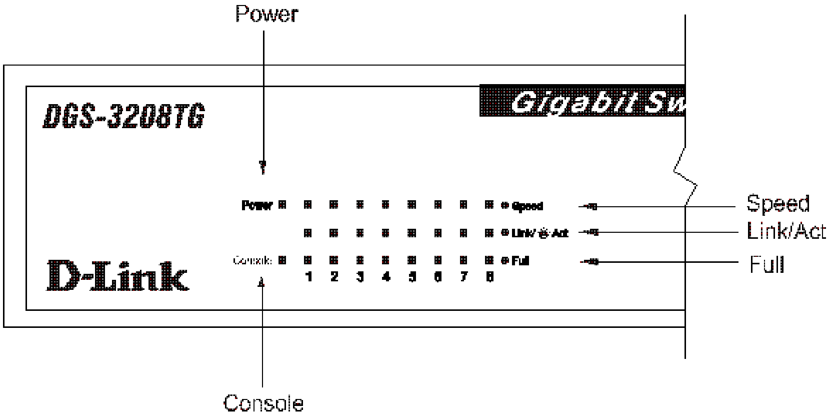


**Figure 3-4. The DGS-3208TG Switch LED indicators**

- **Power** After turning on the power, the Power indicator on the front panel should light to indicate the Switch is loading onboard software. This indicator should then remain on to indicate the ready state of the Switch.

- **Console** This LED indicator is lit 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. When a secured connection is established, this LED indicator is lit. Otherwise, it remains dark.

- **Speed** The interpretation of this LED indicator is dependent on the whether the corresponding port is a GBIC port or a 1000BASE-T port. ***For both GBIC ports:*** The speed LED indicates the port is operational at 1000 Mbps when lit. ***For the 1000BASE-T ports:*** The speed LED indicates the port is operational at 1000 Mbps when lit. When this indicator is not on, the port speed is 100 Mbps.

- **Link/ACT** These LED indicators are lit when there is a secure connection (or link) to a device at any of the ports. The LED indicators blink whenever there is reception or transmission (i.e. Activity—ACT) of data occurring at a port.

- **Full** These LED indicators are illuminated when a port is operating in full-duplex mode.

# 4

# CONNECTING THE SWITCH

This chapter describes how to connect the DGS-3208TG to your Gigabit Ethernet network.

## PC to Switch

A PC can be connected to the Switch via a four-pair Category 5 cable or a fiber optic cable. The PC should be connected to any of the eight ports of the DGS-3208TG.

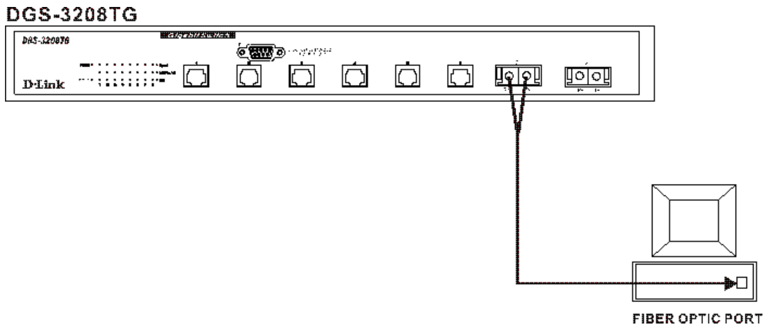


**Figure 4-1. DGS-3208TG Switch connected to a PC or Workstation (full-duplex mode is required)**

The LED indicators for PC connection are dependent on the LAN card capabilities. If LED indicators are not illuminated after making a proper connection, check the PC’s LAN card, the cable, Switch conditions, and connections.

The following are LED indicator possibilities for a PC to Switch connection:

♦ The Link/ACT LED indicator lights up upon hookup.

## Switch to Switch (other devices)

The Switch can be connected to another switch or other devices (routers, bridges, etc.) via a fiber optic cable.

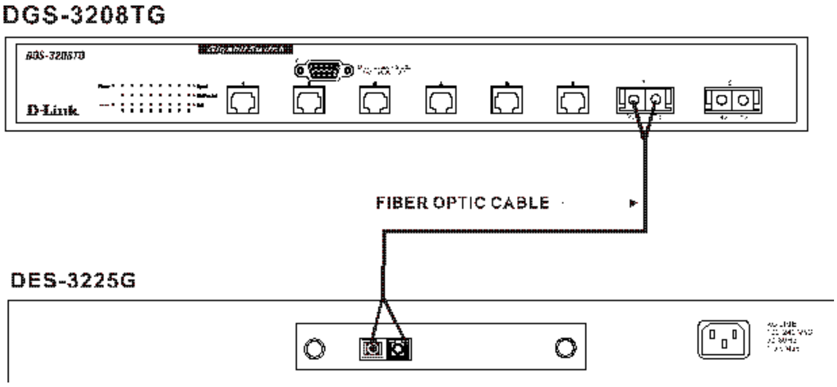


Figure 4-2.  DGS-3208TG Switch to switch connection.

# 5

# SWITCH MANAGEMENT CONCEPTS

## Local Console Management

Local console management involves the administration of the DGS-3208TG Switch via a direct connection to the RS-232 DCE console port. From the Main Menu screen of the console program, an Administrator or Normal User (defined in the next chapter) has privilege and access to manage, control, and monitor the many functions of the Switch.

The components of the Switch allow them to be part of a manageable network. These components include a CPU, memory for data storage, other related hardware, and the SNMP agent firmware. Activities on the Switch can be monitored with these components, while the Switch can be manipulated to carry out specific tasks.

Out-of-band management for the Switch is accomplished through a locally connected management terminal to the RS-232 console port. Through this port, a user can set up, monitor, or change the configuration of the Switch.

The Spanning Tree Algorithm (STA) provides the capability for the Switch to operate properly with other Bridges in a SNMP network supporting the STA. Using the STA, the network will prevent network loop, and automatically establish and activate a backup path in the event of a path failure.

### Console port (RS-232 DCE)

Out-of-band management requires connecting a PC (with a SNMP management platform) to the RS-232 DCE console port of the Switch. Switch management using terminal emulation/VT100 when connected to the RS-232 DCE console port is called *Local Console Management* to differentiate it from management done via management platforms.

The console port is set for the following configuration:

| | | |
|---|---|---|
| ◊ | Baud rate: | 9,600 |
| ◊ | Parity: | none |
| ◊ | Data width: | 8 bits |
| ◊ | Stop bits | 1 |

### IP Addresses and SNMP Community Names

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

In addition, you can also set in the Switch an IP Address for a gateway or a router. It is useful when the management station is not located on the same network as the Switch, making it necessary for the Switch to go through a gateway or router to reach the network manager.

For security, you can set in the Switch a list of IP Addresses of the network managers that you allow to manage the Switch. You can also change the default Community Name in the Switch and set access rights of these Community Names.

## Traps

Trap managers are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap managers can receive traps sent from the Switch; they must immediately take certain actions to avoid future failure or breakdown of the network.

Traps are messages that alert you 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 network manager (trap managers). The following lists the types of events that can take place on the Switch.

- ◊ System resets
- ◊ Errors
- ◊ Status changes
- ◊ Topology changes
- ◊ Operation

You can also specify which network managers may receive traps from the Switch by setting a list of IP Addresses of the authorized network managers.

The following are trap types a trap manager will receive:

- ♦ **Cold Start** This trap signifies that the Switch has been powered up and initialized such that software settings are reconfigured and hardware systems are rebooted. A cold start is different from a factory reset.

- ♦ **Warm Start** This trap signifies that the Switch has been rebooted, however the POST (Power On Self-Test) is skipped.

- ♦ **Authentication Failure** This trap signifies that an addressee (or manager/user) on the Switch is not a valid user of the Switch and may have entered an incorrect community name.

- ♦ **New Root** This trap indicates that the Switch has become the new root of the Spanning Tree, the trap is sent by a bridge soon after its election as the new root. This implies that upon expiration of the Topology Change Timer the new root trap is sent out immediately after the Switch's selection as a new root.

- ♦ **Topology Change** A Topology Change trap is sent by the Switch when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a new root trap is sent for the same transition.

- ♦ **Link Change Event** This trap is sent whenever the link of a port changes from link up to link down or from link down to link up.

## MIBs

The information stored in the Switch is known as the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, MIB values inside the Switch can be retrieved from any SNMP-based network manager. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. These MIBs may also be retrieved by specifying the MIB's Object-Identity (OID) at the network manager. MIB values can be either read-only or read-write.

Read-only MIBs variables can be either constants that are programmed into the Switch, or variables that change while the Switch is in operation. Examples of read-only constants are the number of ports and types of ports. Examples of read-only variables are the statistics counters such as the number of errors that have occurred, or how many kilobytes of data have been received and forwarded through a port.

Read-write MIBs are variables usually related to user-customized configurations. Examples of these are the Switch's IP Address, Spanning Tree Algorithm parameters, and port status.

If you use a third-party vendors' SNMP software to manage the Switch, a diskette listing the Switch's propriety enterprise MIBs can be obtained by request. If your software provides functions to browse or modify MIBs, you can also get the MIB values and change them (if the MIBs' attributes permit the write operation). This process however can be quite involved, since you must know the MIB OIDs and retrieve them one by one.

## Packet Forwarding

The Switch looks at the network configuration to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all segments, are transmitted to the destination only. Example: if Port 1 receives a packet destined for Port 2, the Switch transmits that packet through Port 2 only, and transmits nothing through Port 1.

- **Filtering Database** A Switch filters frames, i.e., does not relay frames received by a Switch port to other ports on that Switch, in order to prevent the duplication of frames. Frames transmitted between a pair of end stations can be confined to LANs that form a path between those end stations.

The functions that support the use and maintenance of filtering database information are:

1. Permanent configuration of reserved addresses.

2. Explicit configuration of static filtering information.

3. Automatic learning of dynamic filtering information through observation of Switched Local Area Network traffic.

4. Aging out of filtering information that has been automatically learned.

5. Calculation and configuration of Switched Local Area Network topology.

## Aging Time

The Aging Time is a parameter that affects the auto-learn process of the Switch in terms of the network configuration. Dynamic Entries, which make up the auto-learned-node address, are aged out of the address table according to the Aging Time that you set.

The Aging Time can be from 10 to 1,000,000 seconds. A very long Aging Time can result with the out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions.

In the opposite case, if the Aging Time is too short, many entries may be aged out soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table.

## *Spanning Tree Algorithm*

The Spanning Tree Algorithm (STA) in the Switch allows you to create alternative paths (with multiple switches or other types of bridges) in your network. These backup paths are idle until the Switch determines that a problem has developed in the primary paths. When a primary path is lost, the switch providing the alternative path will automatically go into service with no operator intervention. This automatic network reconfiguration provides maximum uptime to network users. The concept of the Spanning Tree Algorithm is a complicated and complex subject and must be fully researched and understood. Please read the following before making any changes.

- **Network loop detection and prevention** With STA, there will be only one path between any two LANs. If there is more than one path, forwarded packets will loop indefinitely. STA detects any looped path and selects the path with the lowest path cost as the active path, while blocking the other path and using it as the backup path.

- **Automatic topology re-configuration** When the path for which there is a backup path fails, the backup path will be automatically activated, and STA will automatically re-configure the network topology.

## *STA Operation Levels*

STA operates on two levels: the bridge level and the port level. On the bridge level, STA calculates the Bridge Identifier for each Switch, then sets the Root Bridge and the Designated Bridges. On the port level, STA sets the Root Port and Designated Ports. Details are as follows:

### On the Bridge Level

- **Root Bridge** The switch with the lowest Bridge Identifier is the Root Bridge. Naturally, you will want the Root Bridge to be the best switch among the switches in the loop to ensure the highest network performance and reliability.

- **Bridge Identifier** This is the combination of the Bridge Priority (a parameter that you can set) and the MAC address of the switch. Example: 4 00 80 C8 00 01 00, where 4 is the Bridge Priority. A lower Bridge Identifier results in a higher priority for the switch, and thus increases it probably of being selected as the Root Bridge.

- **Designated Bridge** From each LAN segment, the attached Bridge that has the lowest Root Path Cost to the Root Bridge is the Designated Bridge. It forwards data packets for that LAN segment. In cases where all Switches have the same Root Path Cost, the switch with the lowest Bridge Identifier becomes the Designated Bridge.

- **Root Path Cost** The Root Path Cost of a switch is the sum of the Path Cost of the Root Port and the Root Path Costs of all the switches that the packet goes through. The Root Path Cost of the Root Bridge is zero.

- **Bridge Priority** This is a parameter that users can set. The smaller the number you set, the higher the Bridge Priority is. The higher the Bridge Priority, the better the chance the Switch will be selected as the Root Bridge.

### On the Port Level

- **Root Port** Each switch has a Root Port. This is the port that has the lowest Path Cost to the Root Bridge. In case there are several such ports, then the one with the lowest Port Identifier is the Root Port.
- **Designated Port** This is the port on each Designated Bridge that is attached to the LAN segment for which the switch is the Designated Bridge.
- **Port Priority** The smaller this number, the higher the Port Priority is. With higher Port Priority, the higher the probability that the port will be selected as the Root Port.
- **Path Cost** This is a changeable parameter and may be modified according to the STA specification.

## *User-Changeable Parameters*

The factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory, unless it is absolutely necessary. The user-changeable parameters in the Switch are as follows:

- **Bridge Priority** A Bridge Priority can be from 0 to 65535. 0 is equal to the highest Bridge Priority.
- **Bridge Hello Time** The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge. (Note that the Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur).
- **Bridge Max. Age** The Max. Age can be 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 Forward Delay** 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.

  Observe the following formulas when you set the above parameters:

  1. Max. Age = 2 x (Forward Delay - 1 second)
  2. Max. Age = 2 x (Hello Time + 1 second)

- **Port Priority** A Port Priority can be from 0 to 255. The lower the number, the greater the probability the port will be chosen as the Root Port.

## *Illustration of STA*

A simple illustration of three Bridges (or the Switch) connected in a loop is depicted in *Figure 5-1*. In this example, you can anticipate some major network problems if the STA assistance is not applied. For instance, if Bridge 1 broadcasts a packet to Bridge 2, Bridge 2 will broadcast it to Bridge 3, Bridge 3 will broadcast it to Bridge 1, and so on. The broadcast packet will be passed indefinitely in a loop, causing a serious network failure.

To alleviate network loop problems, STA can be applied as shown in *Figure* 5-2. In this example, STA breaks the loop by blocking the connection between Bridge 1 and 2. The decision to block a particular connection is based on the STA calculation of the most current Bridge and Port settings. Now, if Bridge 1 broadcasts a packet to Bridge 3, then Bridge 3 will broadcast it to Bridge 2 and the broadcast will end there.

STA setup can be somewhat complex. Therefore, you are advised to keep the default factory settings and STA will automatically assign root bridges/ports and block loop connections. However, if you need to customize the STA parameters, refer to *Table 5-1*.

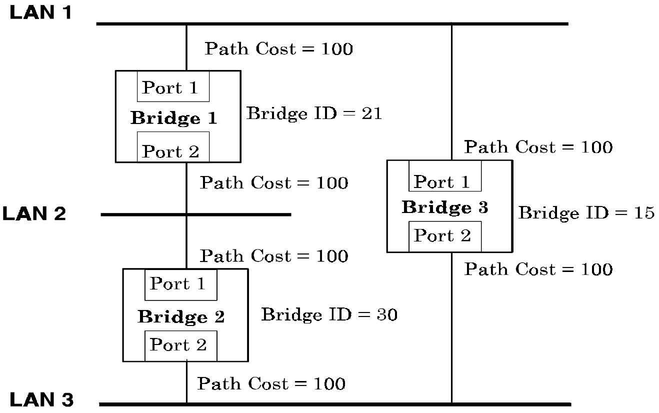


**Figure 5-1. Before Applying the STA Rules**

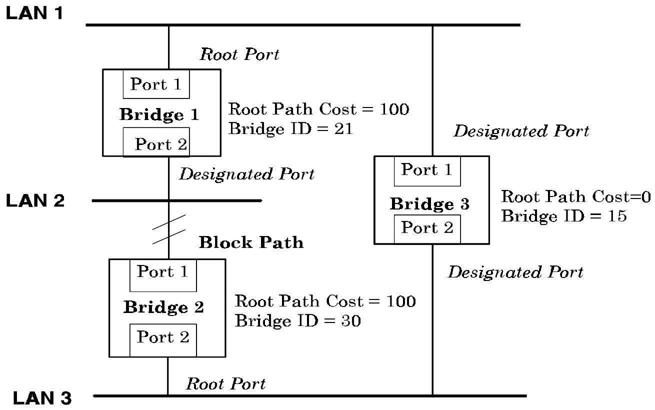


**Figure 5-2. After Applying the STA Rules**

| STA parameters | Settings | Effects | Comment |
|---|---|---|---|
| **Bridge Priority** | lower the #, higher the priority | Increases chance of becoming the Root Bridge | Avoid, if the switch is used in workgroup level of a large network |
| **Hello Time** | 1 - 10 sec. | No effect, if not Root Bridge | Never set greater than Max. Age Time |
| **Max. Age Time** | 6 - 40 sec. | Compete for Root Bridge, if BPDU is not received | Avoid low number for unnecessary reset of Root Bridge |
| **Forward Delay** | 4 - 30 sec. | High # delays the change in state | Max. Age ≤ 2 x (Forward Delay - 1)<br>Max. Age ≥ 2 x (Hello Time + 1) |
| **Port-level STA parameters** | | | |
| **Enable/Disable** | Enable/<br>Disable | Enable or disable this LAN segment | Disable a port for security or problem isolation |
| **Port Priority** | lower the #, higher the priority | Increases chance of become Root Port | |

Table 5-1. User-selective STA parameters

## Port Trunking

Port trunking is used to combine a number of ports together to make a single high-bandwidth data pipeline. The participating parts are called members of a trunk group.

The Switch supports up to four trunk groups, the first three which may include from two to four switch ports each. The fourth trunk group is two ports.

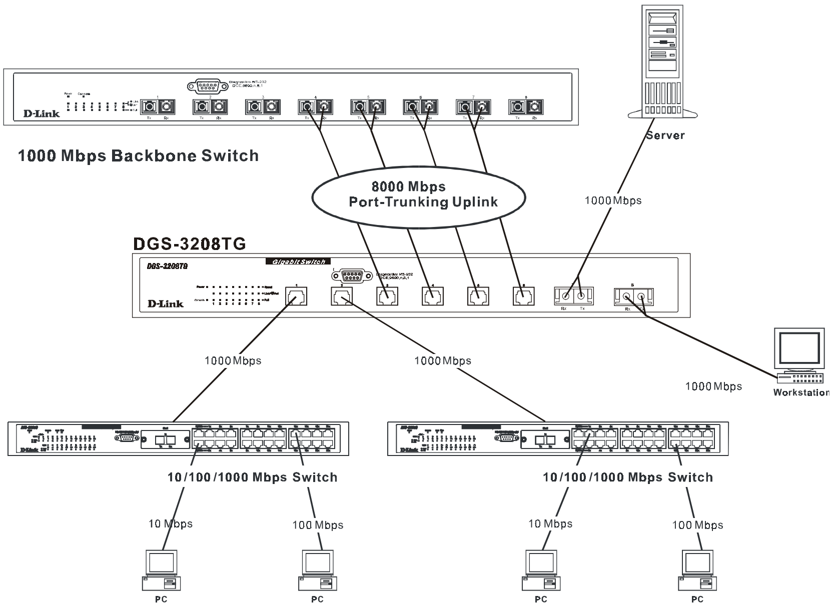


Figure 5-3. Port trunking example

The switch treats all ports in a trunk group as a single port. As such, trunk ports will not be blocked by the spanning tree algorithm.

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

## *VLANs & MAC-based Broadcast Domains*

VLANs are a collection of users or switch ports grouped together in a secure, autonomous broadcast and multicast domain. The main purpose of setting up VLANs or a broadcast domain on a network is to limit the range and effects of broadcast packets.

Two types of VLANs are implemented on the Switch: 802.1Q VLANs and port-based VLANs. MAC-based broadcast domains are a third option. Only one type of VLAN or broadcast domain can be active on the Switch at any given time, however. Thus, you will need to choose the type of VLAN or broadcast domain you wish to setup on your network and configure the Switch accordingly. 802.1Q VLANs support IEEE 802.1Q tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant). In contrast, MAC-based broadcast domains are limited to the Switch and devices directly connected to them.

All VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All broadcast, multicast, and unknown packets entering the Switch on a particular VLAN will only be forwarded to the stations or ports (802.1Q and port-based) that are members of that VLAN. 802.1Q and port-based VLANs also limit unicast packets to members of the VLAN, thus providing a degree of security to your network.

Another benefit of 802.1Q and port-based VLANs is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN (the sales VLAN, for example) to another VLAN (the marketing VLAN). This allows VLANs to accommodate network moves, changes and additions with the utmost flexibility. MAC-based broadcast domains, on the other hand, allow a station to be physically moved yet still belong to the same broadcast domain without having to change and configuration settings.

The *untagging* feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The *tagging* feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally (BPDU packets are not tagged).

## *MAC-Based Broadcast Domains*

The Switch supports up to 12 MAC-based broadcast domains, which are by their nature, limited to the Switch itself and the devices connected directly to it.

Since MAC addresses are hard-wired into a station's network interface card (NIC), MAC-based broadcast domains enable network managers to move a station to a different physical location on the network and have that station automatically retain its broadcast domain membership. This provides the network with a high degree of flexibility since even notebook PC's can plug into any available port on a network and communicate with the same people and use the same resources that have been allocated to the broadcast domain in which it is a member.

Since MAC-based broadcast domains do not restrict the transmission of known unicast frames to other broadcast domains, they can only be used to define limited broadcast domains. As such, they are best implemented on networks where stations are frequently moving, for example where people using notebook PCs are constantly plugging into different parts of the network.

Setting up MAC-based broadcast domains is a relatively straightforward process. Simply create the broadcast domain by assigning it a name (description) and add MAC addresses for the stations that will be members.

# *IEEE 802.1Q VLANs*

The Switch supports about 2000 802.1Q VLANs. 802.1Q VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

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

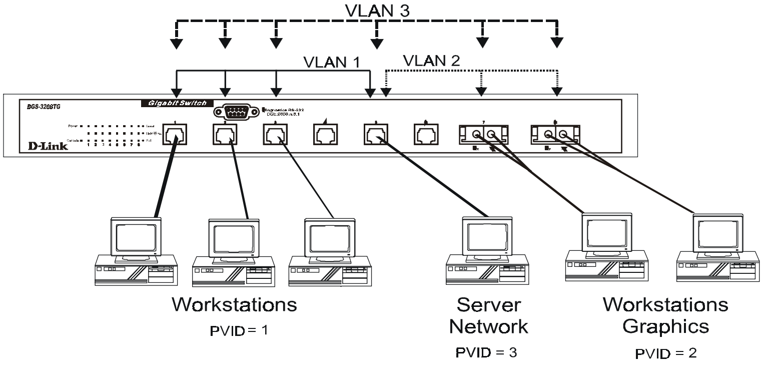
There are two key components to understanding 802.1Q VLANs: Port VLAN ID numbers (PVIDs) and VLAN ID numbers (VIDs). Both variables are assigned to a switch port, but there are important differences between them. A user can only assign one PVID to each switch port. The PVID defines which VLAN a packet belongs to when packets need to be forwarded to another switch port or somewhere else on the network. On the other hand, a user can define a port as a member of multiple VLANs (VIDs), allowing the segment connected to it to receive packets from many VLANs on the network. These two variables control a port’s ability to transmit and receive VLAN traffic, and the difference between them provides network segmentation, while still allowing resources to be shared across more than one VLAN.

## 802.1Q VLAN Segmentation

The following example is helpful in explaining how 802.1Q VLAN segmentation works. Take a packet that is transmitted by a machine on Port 7 that is a member of VLAN 2 and has the Port VLAN ID number 2 (PVID=2). If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 5) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If port 5 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 5 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 7 will only transmit on VLAN 2, because it’s Port VLAN ID number is 2 (PVID=2).

## Sharing Resources Across 802.1Q VLANs

Network resources such as printers and servers however, can be shared across 802.1Q VLANs. This is achieved by setting up overlapping VLANs as shown in the diagram below:



.Figure 5-4. Example of typical VLAN configuration

In the above example, there are three different 802.1Q VLANs and each port can transmit packets on one of them according to their Port VLAN ID (PVID). However, a port can receive packets on all VLANs (VID) that it belongs to. The assignments are as follows:

| ***PVID (Port VLAN ID)*** | ***Ports*** |
|---|---|
| 1 | Port 1 |
| 1 | Port 2 |
| 1 | Port 3 |
| 2 | Port 7 |
| 2 | Port 8 |
| 3 | Port 5 |

| ***VID (VLAN ID)*** | ***Member Ports*** |
|---|---|
| 1 | 1, 2, 3, 5 |
| 2 | 5, 7, 8 |
| 3 | 1, 2, 3, 5, 7, 8 |

Table 5-2. VLAN assignments for Figure 5-4

The server attached to Port 5 is shared by VLAN 1, VLAN 2, and VLAN 3 because Port 5 is a member of all three VLANs (it is listed as a member of VID 1, 2, and 3). Since it can receive packets from all three VLANs, all ports can successfully send packets to it to be printed. Ports 1, 2 and 3 send these packets on VLAN 1 (their PVID=1), and Ports 7 and 8 send these packets on VLAN 2 (PVID=2). The third VLAN (PVID=3) is used by the server to transmit files that had been requested on VLAN 1 or 2 back to the computers. All computers that use the server will receive transmissions from it since they are all located on ports which are members of VLAN 3 (VID=3).

## 802.1Q VLANs Spanning Multiple Switches

802.1Q VLANs can span multiple switches as well as your entire network. Two considerations to keep in mind while building VLANs of this sort are whether the switches are IEEE 802.1Q-compliant and whether VLAN packets should be tagged or untagged.

Definitions of relevant terms are as follows:

- **Tagging** The act of putting 802.1Q VLAN information into the header of a packet. Ports with tagging enabled will put the VID number, priority, and other VLAN information into all packets that flow out it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Tagging is used to send packets from one 802.1Q-compliant device to another.

- **Untagging** The act of stripping 802.1Q VLAN information out of the packet header. Ports with untagging enabled will take all VLAN information out of all packets that flow out of a port. If the packet doesn't have a VLAN tag, the port will not alter the packet, thus keeping the packet free of VLAN information. Untagging is used to send packets from an 802.1Q-compliant switch to a non-compliant device.

- **Ingress port** A port on a switch where packets are flowing into the switch. If an ingress port has the Ingress Filter enabled, the switch will examine each packet to determine whether or not it is a VLAN member and then take one of two actions: if the port is not a member of a VLAN, the packet will be dropped; if the port is a member of a VLAN, then the packet will be forwarded. Otherwise, if the Ingress Filter is disabled, then the switch will process any packet received at this port in its normal fashion.

- **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. If an egress port is connected to an 802.1Q-compliant switch, tagging should be enabled so the other device can take VLAN data into account when making forwarding decisions (this allows VLANs to span multiple switches). If an egress connection is to a non-compliant switch or end-station, tags should be stripped so the (now normal Ethernet) packet can be read by the receiving device.

### *VLANs Over 802.1Q-compliant Switches*

When switches maintaining the same VLANs are 802.1Q-compliant, it is possible to use tagging. Tagging puts 802.1Q VLAN information into each packet header, enabling other 802.1Q-compliant switches that receive the packet to know how to treat it. Upon receiving a tagged packet, an 802.1Q-compliant switch can use the information in the packet header to maintain the integrity of VLANs, carry out priority forwarding, etc.

Data transmissions between 802.1Q-compliant switches take place as shown below.

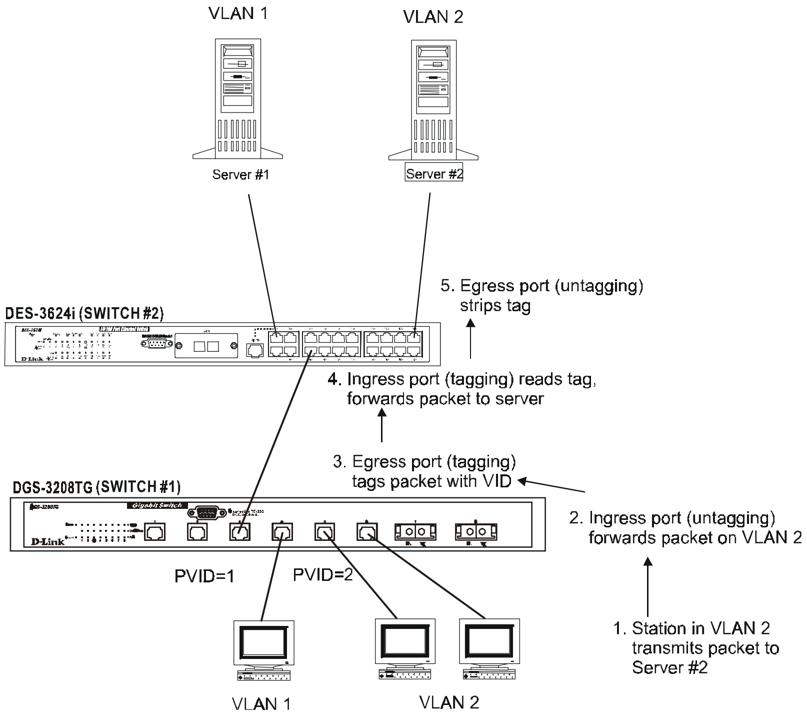

VLAN 1
VLAN 2
Server #1
Server #2
5. Egress port (untagging) strips tag
DES-3624i (SWITCH #2)
4. Ingress port (tagging) reads tag, forwards packet to server
3. Egress port (tagging) tags packet with VID
DGS-3208TG (SWITCH #1)
2. Ingress port (untagging) forwards packet on VLAN 2
PVID=1
PVID=2
1. Station in VLAN 2 transmits packet to Server #2
VLAN 1
VLAN 2

**Figure 5-5. Data transmissions between 802.1Q-compliant Switches**

In the above example, step 4 is the key element. Because the packet has 802.1Q VLAN data encoded in its header, the ingress port can make VLAN-based decisions about its delivery: whether server #2 is attached to a port that is a member of VLAN 2 and, thus, should the packet be delivered; the queuing priority to give to the packet, etc. It can also perform these functions for VLAN 1 packets as well, and, in fact, for any tagged packet it receives regardless of the VLAN number.

If the ingress port in step 4 were connected to a non-802.1Q-compliant device and was thus receiving untagged packets, it would tag its own PVID onto the packet and use this information to make forwarding decisions. As a result, the packets coming from the non-compliant device would automatically be placed on the ingress ports VLAN and could only communicate with other ports that are members of this VLAN.

## *Port-Based VLANs*

Port-based VLANs are a simplified version of the 802.1Q VLANs described in the previous section. In port-based VLANs, all the 802.1Q settings are pre-configured allowing you to quickly and easily setup and maintain port-based VLANs on your network.

In port-based VLANs, broadcast, multicast and unknown packets will be limited to within the VLAN. Thus, port-based VLANs effectively segment your network into broadcast domains. Furthermore, ports can only belong to a single VLAN.

Because port-based VLANs are uncomplicated and fairly rigid in their implementation, they are best used for network administrators who wish to quickly and easily setup VLANs in order to isolate limit the effect of broadcast packets on their network.

For the most secure implementation, make sure that end stations are directly connected to the switch. Attaching a hub, switch or other repeater to the port causes all stations attached to the repeater to become members of the port-based VLAN.

To setup port-based VLANs, simply select a VLAN ID number, name the VLAN, and specify which ports will be members. All other ports will automatically be forbidden membership, even dynamically as a port can belong to only one VLAN.

# Broadcast Storms

Broadcast storms are a common problem on today's networks. Basically, they consist of broadcast packets that flood and/or are looped on a network causing noticeable performance degradation and, in extreme cases, network failure. Broadcast storms can be caused by network loops, malfunctioning NICs, bad cable connections, and applications or protocols that generate broadcast traffic, among others.

In effect, broadcast storms can originate from any number of sources, and once they are started, they can be self-perpetuating, and can even multiply the number of broadcast packets on the network over time. In the best case, network utilization will be high and bandwidth limited until the hop counts for all broadcast packets have expired, whereupon the packets will be discarded and the network will return to normal. In the worst case, they will multiply, eventually using up all the network bandwidth (although network applications will usually crash long before this happens), and cause a network meltdown.

Broadcast storms have long been a concern for network administrators with routers traditionally being used to prevent their occurrence, and if that failed, to at least limit their scope. However, with the advent of VLANs, switches are now able to limit broadcast domains better and cheaper than routers. Also, many switches, including the DGS-3208TG, have broadcast sensors and filters built into each port to further control broadcast storms.

## *Segmenting Broadcast Domains*

The Switch allows you to segment broadcast domains. It does this by forwarding packets only to ports in the same broadcast domain or VLAN. Thus, broadcast packets will only be forwarded to ports that are members of the same broadcast domain or VLAN. Other parts of the network are effectively shielded. As a result, the smaller the broadcast domain, the less effect a broadcast storm will have. Since VLANs and broadcast domains are implemented at each switch port, they can be quite effective in limiting the scope of broadcast storms.

## Eliminating Broadcast Storms

SNMP agents can be programmed to monitor the number of broadcast packets on switch ports and act on the data. When the number of broadcast packets on a given port rise past an assigned threshold, an action can be triggered. When enabled, the usual action is to block the port to broadcast frames, which discards all broadcast frames arriving at the port from the attached segment. Not only does this isolate the broadcast domain, but it actually starts removing broadcast packets from the affected segment. When the number of broadcast packets falls to an acceptable level (below a *falling threshold*), the SNMP agent can remove the blocking condition, returning the port to its normal operational state.

In the Switch, the default rising threshold is met when more than 500 broadcast packets per second are being detected on a specified port. Once the rising threshold is surpassed for a duration of more than 5 seconds, it will trigger the broadcast storm rising action configured by the user. The default falling threshold is met if there are less than 250 broadcast packets per second. It is triggered once the duration is at least 30 seconds. The actions can easily be defined by using a normal SNMP management program or through the console interface.

# 6

# USING THE CONSOLE INTERFACE

Your Gigabit Ethernet Switch supports a console management interface that allows you to set up and control your Switch, either with an ordinary terminal (or terminal emulator), or over the network using the TCP/IP Telnet protocol. You can use this facility to perform many basic network management functions. In addition, the console program will allow you to set up the Switch for management using an SNMP-based network management system. This chapter describes how to use the console interface to access the Switch, change its settings, and monitor its operation.

## Setting Up A Console

First-time configuration must be carried out through a “console,” that is, either (a) a VT100-type serial data terminal, or (b) a computer running communications software set to emulate a VT100. The console must be connected to the Diagnostics port. This is an RS-232 port with a 9-socket D-shell connector and DCE-type wiring. Make the connection as follows:

**1.** Obtain suitable cabling for the connection.

You can use either (a) a “null-modem” RS-232 cable or (b) an ordinary RS-232 cable and a null-modem adapter. One end of the cable (or cable/adapter combination) must have a 9-pin D-shell connector suitable for the Diagnostics port; the other end must have a connector suitable for the console’s serial communications port.

**2.** Power down the devices, attach the cable (or cable/adapter combination) to the correct ports, and restore power.

**3.** Set the console to use the following communication parameters for your terminal:

- 9600 baud
- No parity checking (sometimes referred to as “no parity”)
- 8 data bits (sometimes called a “word length” of 8 bits)
- 1 stop bit (sometimes referred to as a 1-bit stop interval)
- VT-100/ANSI compatible
- Arrow keys enabled

A typical console connection is illustrated below:

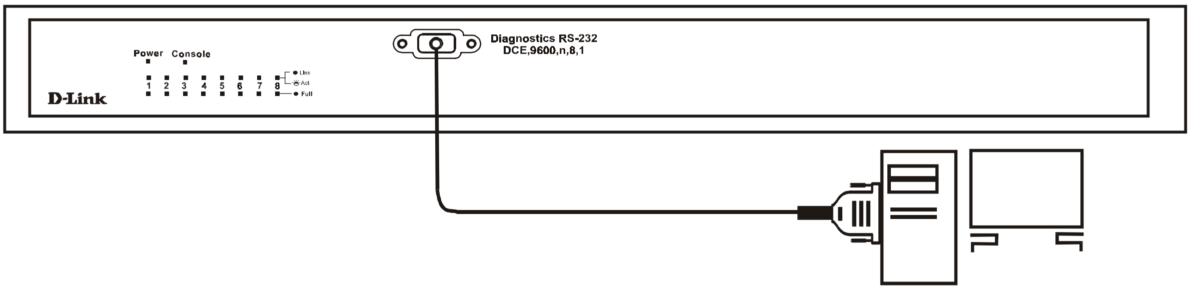


**Figure 6-1. Example of a console connection**

## Connecting to the Switch Using Telnet

Once you have set an IP address for your Switch, you can use a Telnet program (in a VT-100 compatible terminal mode) to access and control the Switch. Most of the screens are identical, whether accessed from the console port or from a Telnet interface. You can also use a Web-based browser to manage the Switch. See the next chapter, *"Web-Based Network Management,"* for further information.

## Console Usage Conventions

The console interface makes use of the following conventions:

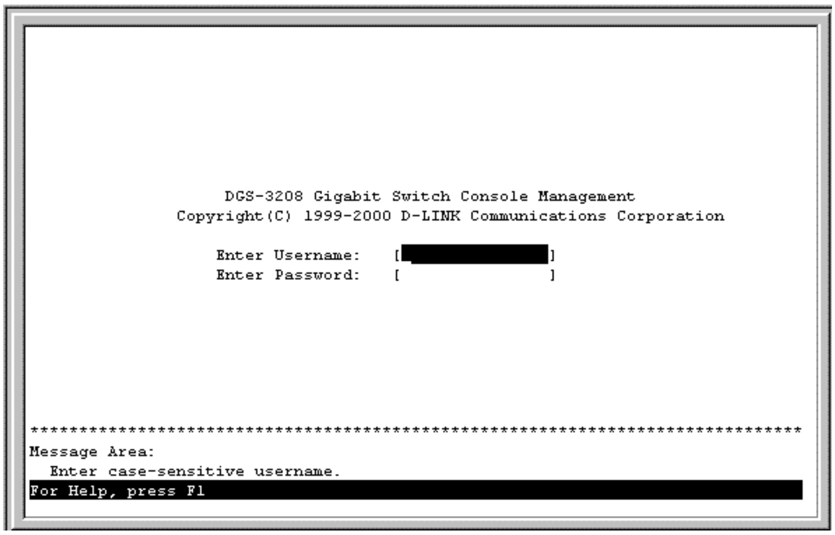
1. Items in **<***angle brackets***>** can be toggled on or off using the space bar, excepting the entries on the Port Configuration screen.
2. Items in [*square brackets*] can be changed by typing in a new value. You can use the backspace and delete keys to erase characters behind and in front of the cursor.
3. The up and down arrow keys, the left and right arrow keys, the tab key and the backspace key, can be used to move between selected items. It is recommended that you use the tab key and backspace key for moving around the console.
4. Items in UPPERCASE are commands. Moving the selection to a command and pressing <Enter> will execute that command, e.g. SAVE, EXIT, etc.

## First Time Connecting To The Switch

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

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

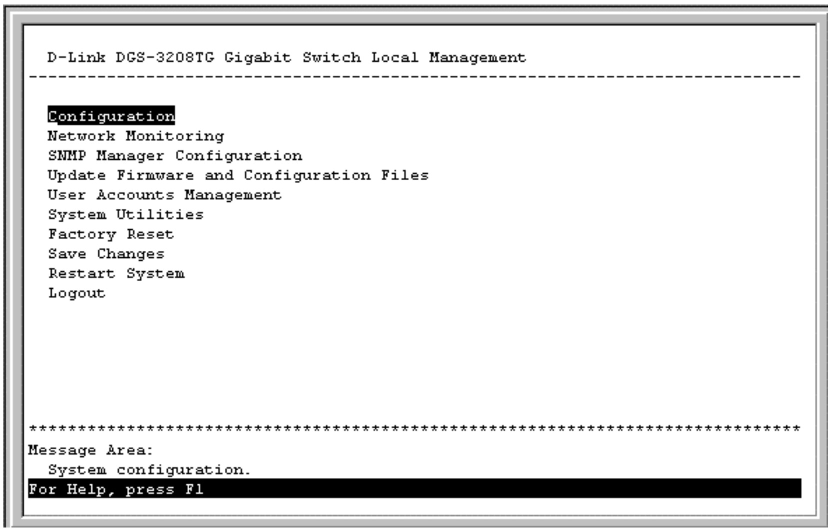
When you first connect to the Switch, you will be presented with the first login screen (shown below). If the initial login screen does not appear, press Ctrl+R (hold down the Ctrl key, press and release the R key, and then release Ctrl) to call up the screen. Ctrl+R can also be used at any time to refresh the screen.



```
                DGS-3208 Gigabit Switch Console Management
           Copyright(C) 1999-2000 D-LINK Communications Corporation

               Enter Username:   [               ]
               Enter Password:   [               ]




*******************************************************************************
Message Area:
  Enter case-sensitive username.
For Help, press F1
```

**Figure 6-2. Initial Screen, first time connecting to the Switch**

Press <Enter> (Note: Leave the Username and Password fields blank). You will see the main menu shown below:



```
  D-Link DGS-3208TG Gigabit Switch Local Management
-------------------------------------------------------------------------------

  Configuration
  Network Monitoring
  SNMP Manager Configuration
  Update Firmware and Configuration Files
  User Accounts Management
  System Utilities
  Factory Reset
  Save Changes
  Restart System
  Logout




*******************************************************************************
Message Area:
  System configuration.
For Help, press F1
```

**Figure 6-3. Main Menu**

The first user automatically gets *Administrator* privileges (See *Table 6-1*). It is recommended to create at least one *Administrator*-level user for the Switch.

## *Steps to Create Administrator or Normal User Access*

From the screen above, move the cursor to **User Accounts Management** and press <Enter>. The **User Account Management** menu appears.

1. Choose **Create/Modify User Accounts** from the **User Account Management** menu. The **Add/Modify User Accounts** menu appears.

2. Enter the new username, assign an initial password, and then confirm the new password. Determine whether the new user should have *Administrator* or *Normal User* privileges. (Use the space bar to toggle between the two options).

3. Press APPLY to let the user addition take effect.

4. Press <Esc> to return to the previous screen or Ctrl+T to go to the root screen.

5. To see a listing of all user accounts and access levels, press <Esc>. Then choose **View/Delete User Accounts**. The **View/Delete User Account** screen appears.

## Administrator and Normal User Privileges

There are two levels of user privileges: *Administrator* and *Normal User*. Some menu selections available to users with *Administrator* privileges may not be available to *Normal User*s. The main menus shown are the menus for the two types of users:

The following table summarizes *Administrator* and *Normal User* privileges:

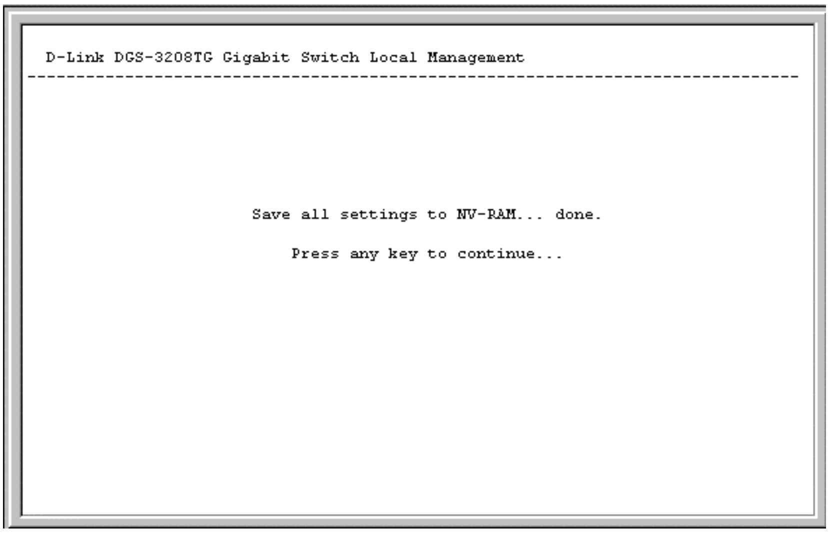
| Menu | Administrator | Normal User |
|---|---|---|
| | Privilege | |
| Configuration | Yes | Yes, view only. |
| Network Monitoring | Yes | Yes, view only. |
| Community Strings and Trap Stations | Yes | Yes, view only. |
| Update Firmware and Configuration Files | Yes | No |
| User Account Management | | |
| Add/Modify User Account | Yes | No |
| View/ Delete User Account | Yes | No |
| System Utilities | Yes | Yes |
| Factory Reset | Yes | No |
| Restart System | Yes | No |

**Table 6-1. Administrator and Normal User Privileges**

After establishing a User Account with *Administrator*-level privileges, press <Esc> twice. Then choose the **Save Changes** menu (seen below). Pressing any key will return to the main menu. You are now ready to operate the Switch.

## Save Changes

In order to retain any modifications made in the current session, it is necessary to choose **Save Changes** from the main menu. The following screen will appear to indicate your new settings have been processed:



```
D-Link DGS-3208TG Gigabit Switch Local Management
--------------------------------------------------------------------------------

                      Save all settings to NV-RAM... done.

                          Press any key to continue...
```

Figure 6-4. Save Changes screen

# Login On The Switch Console By Registered Users

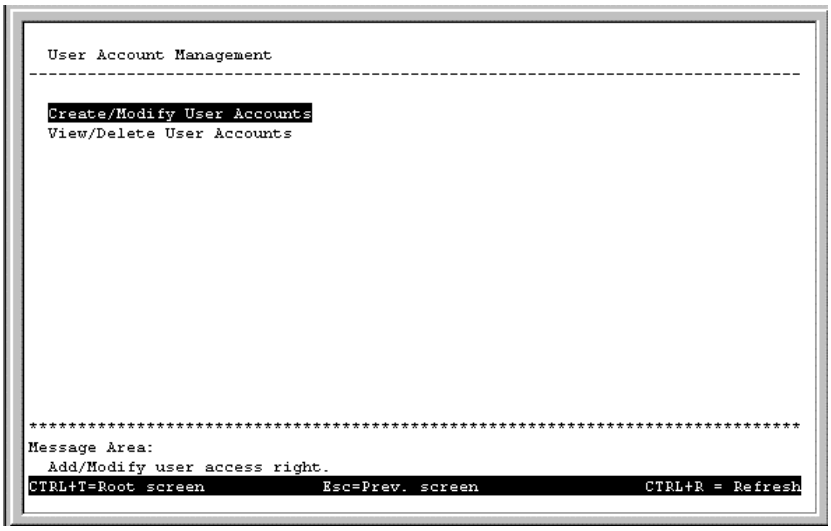
To log in once you have created a registered user,

1. Type in your Username and press <Enter>.
2. Type in your Password and press <Enter>.
3. The main menu screen will be displayed based on your *Administrator* or *Normal User* access level or privilege.

## Add/Modify User Account

To add or change your user password:

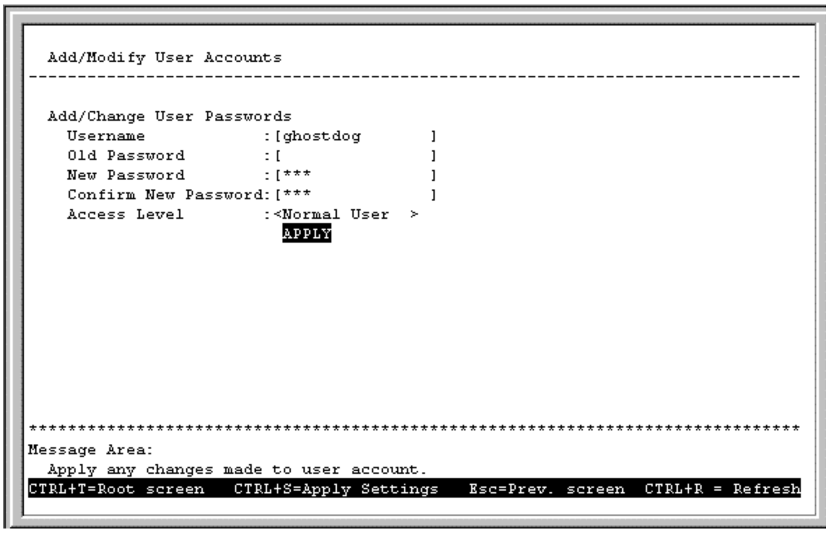
1. Choose **User Accounts Management** from the main menu. The following **User Account Management** menu appears:



```
  User Account Management
-------------------------------------------------------------------------------

  Create/Modify User Accounts
  View/Delete User Accounts













*******************************************************************************
Message Area:
  Add/Modify user access right.
CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

**Figure 6-5. User Account Management menu**

2. Choose **Create/Modify User Account**. The following screen appears:



```
  Add/Modify User Accounts
-------------------------------------------------------------------------------

  Add/Change User Passwords
    Username            :[ghostdog       ]
    Old Password        :[               ]
    New Password        :[***            ]
    Confirm New Password:[***            ]
    Access Level        :<Normal User  >
                          APPLY









*******************************************************************************
Message Area:
  Apply any changes made to user account.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-6. Add/Modify User Accounts screen**

3. Type in your Username and press <Enter>.

4. If you are a new user, type in the Old Password and press <Enter>.

5. Type in the New Password you have chosen, and press <Enter>. Type in the same new password in the following field to verify that you have not mistyped it.

6. Determine whether the new user should have *Normal User* or *Administrator* privileges.

7. Choose the APPLY command to let the password change take effect.

This method can also be used by an *Administrator*-level user to change another user's password.

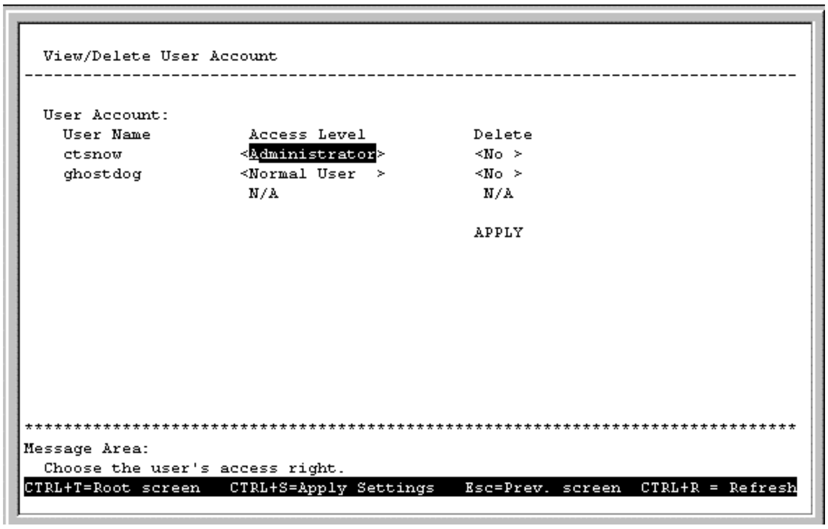
## View/Delete User Account

Access to the console, whether using the console port or via Telnet, is controlled using a user name and password. Up to three user names can be defined. The console interface will not let you delete the current logged-in user, however, in order to prevent accidentally deleting all of the users with *Administrator* privilege.

Only users with the *Administrator* privilege can delete users.

To view your user password:

Choose **View/Delete User Accounts** from the **User Account Management** menu. The following screen appears:



```
 View/Delete User Account
-------------------------------------------------------------------------------

 User Account:
   User Name            Access Level          Delete
   ctsnow              <Administrator>        <No >
   ghostdog            <Normal User  >        <No >
                        N/A                    N/A

                                              APPLY









*******************************************************************************
Message Area:
  Choose the user's access right.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-7. View/Delete User Account screen

To delete your user password:

**1.** Toggle the Delete field of the user you wish to remove to *Yes*.

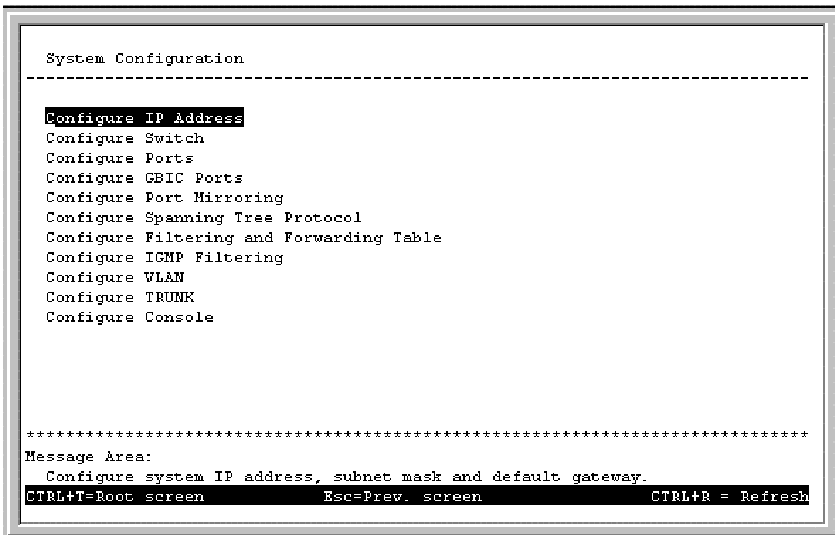
**2.** Press APPLY to let the user deletion take effect.

# Setting Up The Switch

This section will help prepare the Switch user by describing the **System Configuration**, **Firmware and Configuration Update**, **System Utilities,** and **SNMP Configuration** menus and their respective sub-menus.

## System Configuration

Choose **System Configuration** to access the first item on the DGS-3208TG main menu. The following menu appears:



```
  System Configuration
--------------------------------------------------------------------------------

  Configure IP Address
  Configure Switch
  Configure Ports
  Configure GBIC Ports
  Configure Port Mirroring
  Configure Spanning Tree Protocol
  Configure Filtering and Forwarding Table
  Configure IGMP Filtering
  Configure VLAN
  Configure TRUNK
  Configure Console






********************************************************************************
Message Area:
  Configure system IP address, subnet mask and default gateway.
CTRL+T=Root screen            Esc=Prev. screen                  CTRL+R = Refresh
```

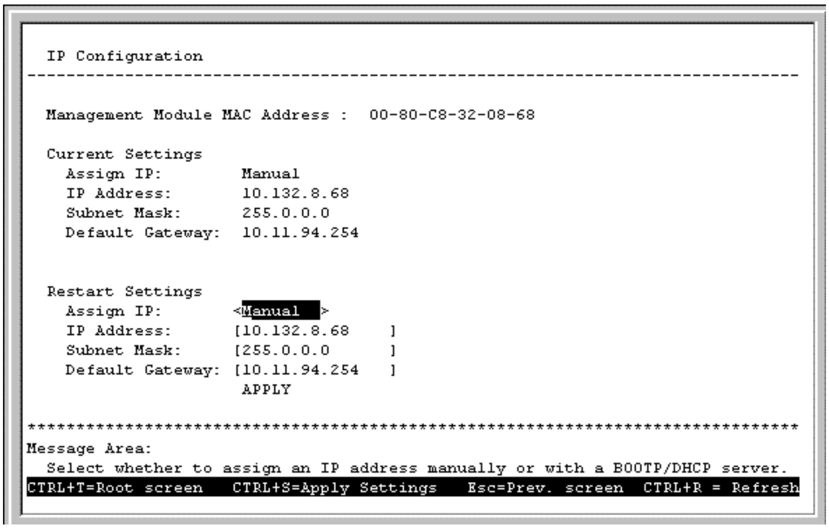
Figure 6-8. System Configuration menu

You will need to change some settings to be able to manage the Switch from an SNMP-based network management system such as SNMP v1 or to be able to access the Switch using the Telnet protocol. See the next chapter for Web-based management information.

## Configure IP Address

The Switch needs to have a TCP/IP address assigned to it so that the network management system or Telnet client can find it on the network. The **IP Configuration** screen allows you to change the settings for the two different interfaces used on the Switch: the Ethernet interface used for in-band communication, and the SLIP interface used over the console port for out-of-band communication.

Choose **Configure IP Address** to access the first item on the **System Configuration** menu. The following screen appears:



```
  IP Configuration
--------------------------------------------------------------------------------

  Management Module MAC Address :  00-80-C8-32-08-68

  Current Settings
    Assign IP:         Manual
    IP Address:        10.132.8.68
    Subnet Mask:       255.0.0.0
    Default Gateway:   10.11.94.254


  Restart Settings
    Assign IP:        <Manual   >
    IP Address:       [10.132.8.68    ]
    Subnet Mask:      [255.0.0.0      ]
    Default Gateway:  [10.11.94.254   ]
                       APPLY

********************************************************************************
Message Area:
  Select whether to assign an IP address manually or with a BOOTP/DHCP server.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen   CTRL+R = Refresh
```

Figure 6-9. IP Configuration screen

Each of the fields on this screen takes effect the next time the system is restarted. Fields that can be set include:

- **Assign IP** Determines whether the Switch should get its IP Address settings from the user (*Manual*), a *BOOTP* server, or a *DHCP* server. If *Manual* is chosen, the Switch will use the IP Address, Subnet Mask and Default Gateway settings defined in this screen upon being rebooted. If *BOOTP* is chosen, 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 supplied settings. If *DHCP* is chosen, a Dynamic Host Configuration Protocol request will be sent when the Switch is powered up.

- **IP Address** Determines the IP address used by the Switch for receiving SNMP and Telnet communications. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. This address should be a unique address on a network assigned to you by the central Internet authorities. The same IP address is shared by both the SLIP and Ethernet network interfaces.

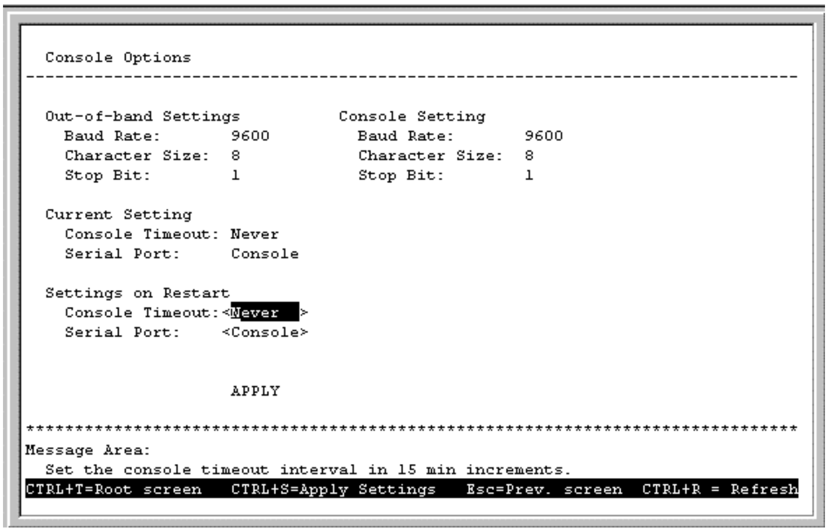
- **Subnet Mask** Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. If no subnetting is being done, the value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network.

- **Default Gateway** IP address that determines where frames with a destination 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 internetwork, or you do not want the Switch to be accessible outside your local network, you can leave this field blank.

## Configure Console

You can use the **Console Options** screen to choose whether to use the Switch's RS-232C serial port for console management or for out-of-band TCP/IP communications using SLIP, and to set the bit rate used for SLIP communications.

Choose **Configure Console** to access the last item on the **System Configuration** menu. The following screen appears:



```
  Console Options
-------------------------------------------------------------------------------

  Out-of-band Settings          Console Setting
    Baud Rate:        9600        Baud Rate:        9600
    Character Size:   8           Character Size:   8
    Stop Bit:         1           Stop Bit:         1

  Current Setting
    Console Timeout: Never
    Serial Port:     Console

  Settings on Restart
    Console Timeout:<Never   >
    Serial Port:    <Console>


                  APPLY

*******************************************************************************
Message Area:
  Set the console timeout interval in 15 min increments.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-10. Console Configuration screen**

The following fields under Settings on Restart can be set:

- **Console Timeout** This setting for the restart of the console is *15 mins*, *30 mins*, *45 mins*, *60 mins*, or *Never*.

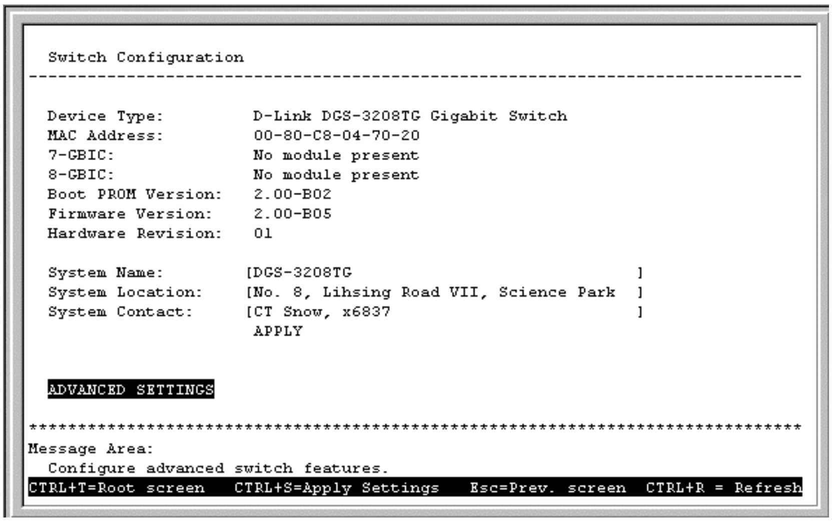
- **Serial Port** Determines whether the serial port should be used for out-of-band (SLIP) management or for console management, starting from the next time the Switch is restarted. In this field, you can toggle between *SLIP* or *Console* port type settings.

- **Baud Rate** Determines the serial port bit rate that will be used the next time the Switch is restarted. Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are *2400*, *9600*, *19200* and *38400* bits per second. The default setting in this Switch version is *9600*.

## Configure Switch

The **Switch Configuration** screen shows various pieces of information about your Switch, and allows you to set the **System Name**, **System Location**, and **System Contact**. These settings can be retrieved from the Switch using SNMP requests, allowing the settings to be used for network management purposes.

Choose **Configure Switch** to access the second item on the **System Configuration** menu. The following screen appears:



```
  Switch Configuration
-------------------------------------------------------------------------------

  Device Type:          D-Link DGS-3208TG Gigabit Switch
  MAC Address:          00-80-C8-04-70-20
  7-GBIC:               No module present
  8-GBIC:               No module present
  Boot PROM Version:    2.00-B02
  Firmware Version:     2.00-B05
  Hardware Revision:    01

  System Name:         [DGS-3208TG                              ]
  System Location:     [No. 8, Lihsing Road VII, Science Park  ]
  System Contact:      [CT Snow, x6837                          ]
                        APPLY


  ADVANCED SETTINGS

*******************************************************************************
Message Area:
  Configure advanced switch features.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-11. Switch Configuration screen**

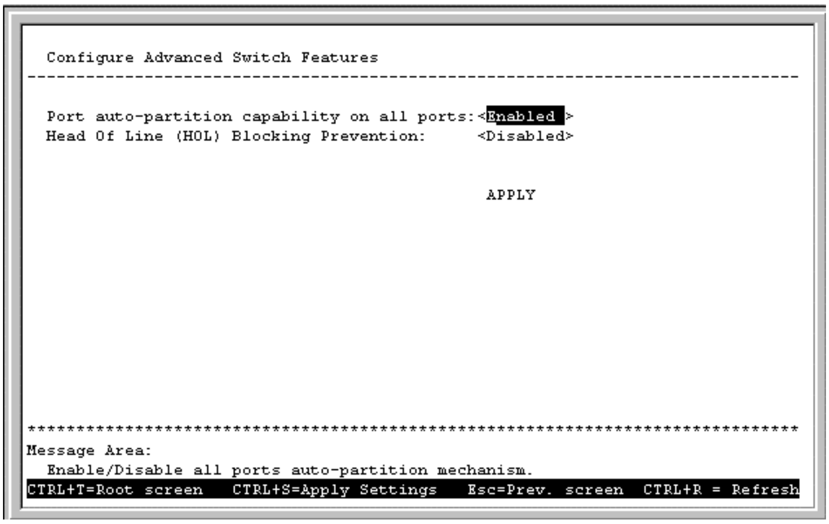
The fields you can set are:

- **System Name** Corresponds to the SNMP MIB II variable `system.sysName`, and is used to give a name to the Switch for administrative purposes. The Switch's fully qualified domain name is often used, provided a name has been assigned.

- **System Location** Corresponds to the SNMP MIB II variable `system.sysLocation`, and is used to indicate the physical location of the Switch for administrative purposes.

- **System Contact** Corresponds to the SNMP MIB II variable `sysContact`, and is used to give the name and contact information for the person responsible for administering the Switch.

The **Configure Advanced Switch Features** screen allows you to enable head of line blocking prevention as well as to partition ports. Press ADVANCE SETTINGS on the **System Configuration** window to access the **Configure Advanced Switch Features** screen:



```
  Configure Advanced Switch Features
--------------------------------------------------------------------------------

  Port auto-partition capability on all ports:<Enabled >
  Head Of Line (HOL) Blocking Prevention:     <Disabled>


                                               APPLY















********************************************************************************
Message Area:
  Enable/Disable all ports auto-partition mechanism.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-12. Configure Advanced Switch Features screen**

The fields you can set are:

- **Port auto-partition capability on all ports** When this function is *Enabled*, if too many consecutive collisions occur on an individual port, the port will be blocked off until a good packet is seen on the wire. If a port is partitioned, the Switch can only transmit data, not receive it.

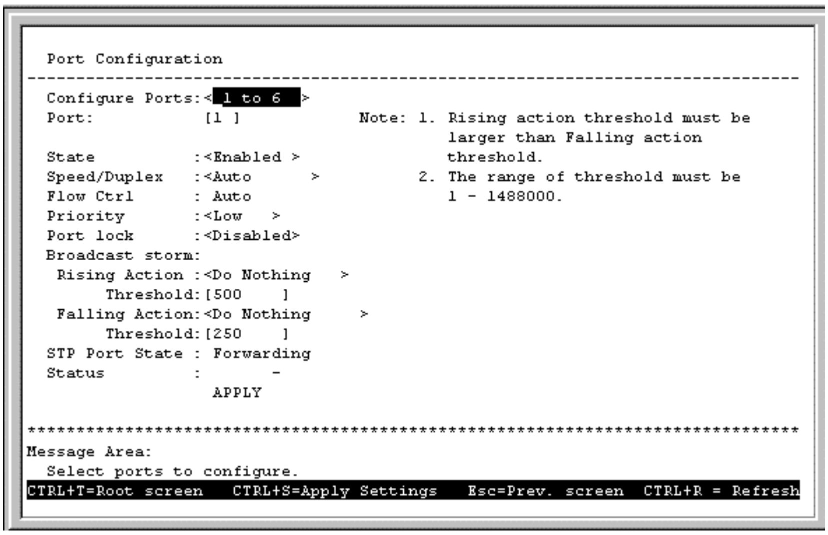
- **Head Of Line (HOL) Blocking Prevention** If *Enabled*, this function is designed to prevent forwarding a packet to a "blocking" port, that is, a port where an excess of packets are queued up. Note that when a multicast packet or a packet with an unknown destination address needs to be forwarded to several ports, and if some of them are "blocking", the packet will not be discarded, rather it will be forwarded only to the ports that are not "blocking."

## Configure Ports

The **Port Configuration** screen allows you to change the port state in the case when you would like to partition a port, or for observation, device repair, or security reasons. Great caution, however, must be observed when partitioning a port; you should make sure that the partitioned port is not being used as the port to control or monitor the condition of other devices.

To change the configuration of a port:

1. Select **System Configuration** from the main menu and then choose **Configure Ports**. The following screen appears:



```
  Port Configuration
-------------------------------------------------------------------------------
  Configure Ports:< 1 to 6  >
  Port:            [1 ]          Note: 1. Rising action threshold must be
                                          larger than Falling action
  State           :<Enabled >              threshold.
  Speed/Duplex    :<Auto      >        2. The range of threshold must be
  Flow Ctrl       : Auto                   1 - 1488000.
  Priority        :<Low   >
  Port lock       :<Disabled>
  Broadcast storm:
   Rising Action :<Do Nothing   >
        Threshold:[500    ]
   Falling Action:<Do Nothing     >
        Threshold:[250    ]
  STP Port State : Forwarding
  Status          :        -
                   APPLY

*******************************************************************************
Message Area:
  Select ports to configure.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-13. Port Configuration screen**

**2.** Specify the port range and specific port in the Configure Ports and Port fields, respectively.

**3.** In the State field, change the port state to *Enabled* or *Disabled*.

**4.** In the Speed/Duplex field, set the speed and duplex mode. Choose from: *1000M/Full*, *100M/Full, 100M/Half,* and *Auto.*

**5.** In the Flow Ctrl field, toggle *Off* or *On*.

**6.** In the Priority field, select *High, Low,* or *Normal.*

**7.** Set Port lock to *Enabled* or *Disabled*.

**8.** In the Broadcast Storm Rising Action and Broadcast Storm Falling Action fields, set the desired settings, including the Thresholds. See below for further explanation.

**9.** Press APPLY and hit <Enter>.

The fields you can set are:

- ♦ **Configure Ports** & **Port** Select the desired port range and the specific port in these fields.
- ♦ **State** When you disable the state, the port will be partitioned from the rest of the network. In this partitioned state, it will only be able to accept management packets. All other packets will be dropped.
- ♦ **Speed/Duplex** When this function is enabled, if too many consecutive collisions occur on an individual port, the port will be blocked off until a good packet is seen on the wire. If a port is partitioned, the Switch can only transmit data, not receive it.
- ♦ **Flow Ctrl** Enables or disables IEEE 802.3x flow control on the port. Flow control allows the port to send a Pause packet to a transmitting IEEE 802.3x-compliant device, so that its buffers don't overflow and data is not lost. Toggles flow control *On* or *Off,* unless Speed/Duplex is set to *Auto,* in which case this setting will also be set to *Auto.*
- ♦ **Priority** Sets the priority for traffic arriving at this port to *High*, *Normal* or *Low*. Higher priority packets are processed first in the Switch's packet queue.

- **Port Lock** When enabled, stops automatic learning for all stations connected to the port. Entries in the Forwarding Table for all devices connected to the port will age out. The only traffic this port will allow is traffic from machines whose MAC addresses are manually entered in the Static Forwarding Table.

- **Broadcast Storm** As a broadcast storm develops, the number of broadcast packets received on a port increases steadily. The Broadcast Storm controls make it possible to (1) prevent a broadcast storm from spreading from one port to others, and (2) restore normal forwarding of broadcast packets when the storm has abated.

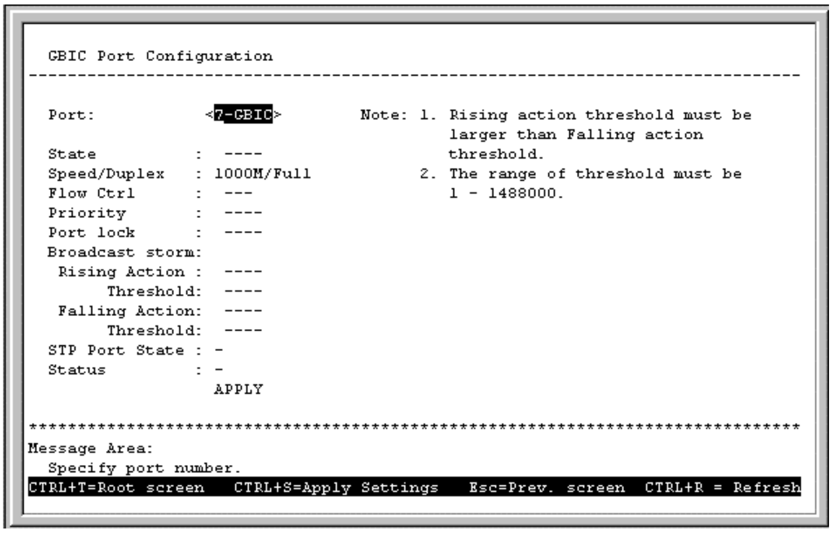
  The Rising Action control and its associated Threshold control specify what action (if any) the Switch should take when broadcast traffic received on the port increases to or exceeds the equivalent of a specified number of broadcast packets per second. The threshold can be set to 1 to 1,488,000 packets per second (the default is 500); the rising action can be set to *Do Nothing* (this is the default), *Block* (that is, discard all broadcast packets received on the port), or *Block & Trap* (discard all broadcast packets received on the port and send a trap to the trap manager[s]).

  The Falling Action control and its associated Threshold control specify what action (if any) the Switch should take when broadcast traffic received on the port, after reaching or exceeding the "rising action" threshold, decreases to or falls below the equivalent of a specified number of broadcast packets per second. The threshold can be set to 1 to 1,488,000 packets per second (the default is 250); the falling action can be set to *Do Nothing* (this is the default), *Forward* (that is, discontinue blocking of broadcast packets received on the port), or *Forward & Trap* (discontinue blocking of broadcast packets received on the port and send a trap to the trap manager[s]).

Press CTRL+S to let the changes take effect. If you wish these changes to be the default for the Switch, return to the main menu and choose **Save Changes**.

STP Port State (whether the Spanning Tree Protocol is enabled or disabled on this port) and Status reflect the current conditions of the port. They are read-only fields and cannot be changed.

## Configure GBIC Ports



```
 GBIC Port Configuration
-------------------------------------------------------------------------------

 Port:            <7-GBIC>        Note: 1. Rising action threshold must be
                                           larger than Falling action
 State          :  ----                    threshold.
 Speed/Duplex   : 1000M/Full             2. The range of threshold must be
 Flow Ctrl      :  ---                     1 - 1488000.
 Priority       :  ----
 Port lock      :  ----
 Broadcast storm:
  Rising Action :  ----
       Threshold:  ----
  Falling Action:  ----
       Threshold:  ----
 STP Port State : -
 Status         : -
                   APPLY

*******************************************************************************
Message Area:
  Specify port number.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

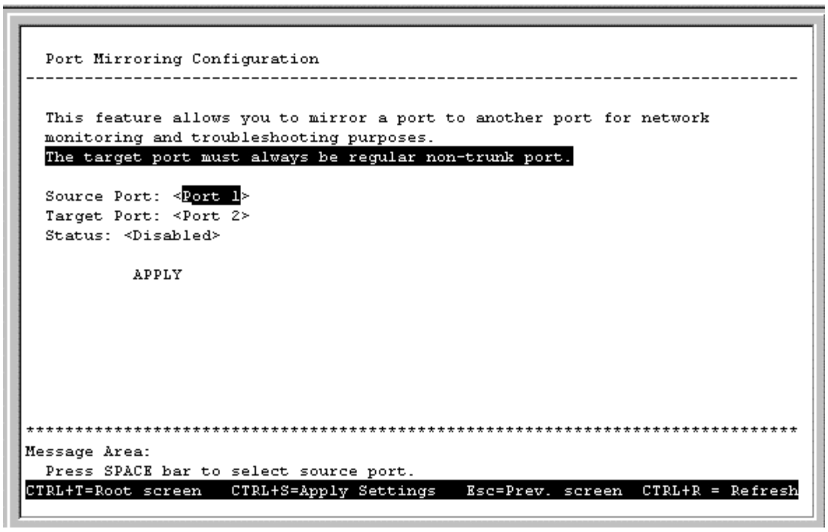
**Figure 6-14. GBIC Port Configuration screen**

See the descriptions for the **Port Configuration** screen in the previous section. Note that on the **GBIC Port Configuration** screen above, Speed/Duplex will always read *1000M/Full*.

## Configure Port Mirroring

The **Port Mirroring Configuration** screen allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

Choose **Configure Port Mirroring** on the **System Configuration** menu to access the **Port Mirroring Configuration** screen:



```
  Port Mirroring Configuration
--------------------------------------------------------------------------------

  This feature allows you to mirror a port to another port for network
  monitoring and troubleshooting purposes.
  The target port must always be regular non-trunk port.

  Source Port: <Port 1>
  Target Port: <Port 2>
  Status: <Disabled>

           APPLY







********************************************************************************
Message Area:
  Press SPACE bar to select source port.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-15. Port Mirroring Configuration screen**

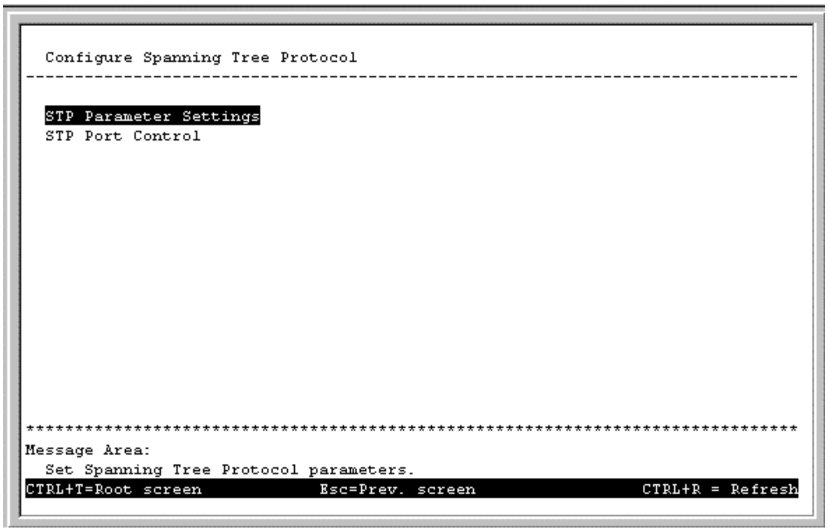
To configure a mirror port, select the port from where you want to copy frames in the Source Port field. Then select the port which receives the copies from the source port in the Target Port field. The target port is where you will connect a monitoring/ troubleshooting device such as a sniffer or an RMON probe. When you are finished, change the Status to *Enabled* and then press APPLY to let your changes take effect.

## Configure Spanning Tree Protocol

The Spanning Tree Algorithm Parameters can be used for creating alternative paths in your network. The Protocol Parameters allow you to change the behind the scene parameters of the Spanning Tree Algorithm at the bridge level. The parameters for this section have been fully explained in Chapter 5's "*Switch Management Concepts*." See *STA Operation Levels: On the Bridge level*, and *User-Changeable Parameters*. It is recommended that you read these sections, as well as the introductory section in the same chapter entitled *Spanning Tree Algorithm* before changing any of the parameters.

To change the Protocol Parameters:

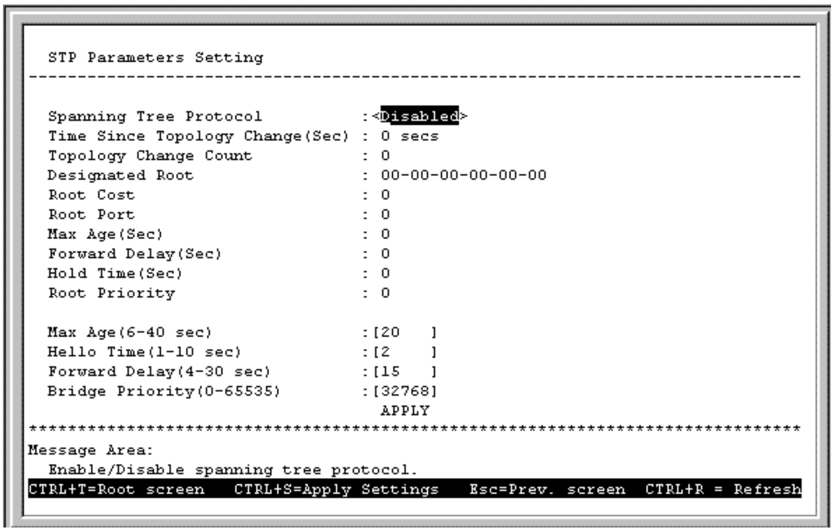
1. Choose **Configure Spanning Tree Protocol** from the **System Configuration** menu. The following **Configure Spanning Tree Protocol** menu will be displayed:



```
  Configure Spanning Tree Protocol
-------------------------------------------------------------------------------

  STP Parameter Settings
  STP Port Control











*******************************************************************************
Message Area:
  Set Spanning Tree Protocol parameters.
CTRL+T=Root screen            Esc=Prev. screen                CTRL+R = Refresh
```

**Figure 6-16. Configure Spanning Tree Protocol menu**

**2.** Choose **STP Parameter Settings** to access the following screen:



```
  STP Parameters Setting
-------------------------------------------------------------------------------

  Spanning Tree Protocol           :<Disabled>
  Time Since Topology Change(Sec)  : 0 secs
  Topology Change Count            : 0
  Designated Root                  : 00-00-00-00-00-00
  Root Cost                        : 0
  Root Port                        : 0
  Max Age(Sec)                     : 0
  Forward Delay(Sec)               : 0
  Hold Time(Sec)                   : 0
  Root Priority                    : 0

  Max Age(6-40 sec)                :[20   ]
  Hello Time(1-10 sec)             :[2    ]
  Forward Delay(4-30 sec)          :[15   ]
  Bridge Priority(0-65535)         :[32768]
                                    APPLY
*******************************************************************************
Message Area:
  Enable/Disable spanning tree protocol.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-17. STP Parameters Setting screen**

**3.** Change the *Disabled* setting to *Enabled* in the Spanning Tree Protocol field.

**4.** Enter the Bridge Max Age in the Max Age(6-40 sec) field.

**5.** Enter the Bridge Hello Time in the Hello Time(1-10 sec) field.

**6.** Enter the Bridge Forward Delay time in the Forward Delay(4-30 sec) field.

**7.** Enter the Bridge Priority in the Bridge Priority(0-65535) field.

**8.** Press APPLY to let your changes take effect.

The information on the screen is described as follows:

♦ **Spanning Tree Protocol** Select *Enabled* to implement the Spanning Tree Protocol.

- **Time Since Topology Changes(sec)** Read-only object displays the last time changes were made to the network topology. These changes usually occur when backup paths are activated due to primary path failures.

- **Topology Change Count** Read-only object displays the number of times (since the current management session with the device was started) changes were made to the network topology. Changes usually occur on the network when backup paths are activated.

- **Designated Root** Read-only object displays the MAC (Ethernet) address of the bridge/switch on the network that has been chosen as the STP root.

- **Root Cost** Read-only object displays the cost for the path between the switch and the root bridge. If the switch is the root bridge, then the root cost is zero.

- **Root Port** Read-only object identifies the port (on the bridge) that offers the least path cost from the bridge to the root bridge. In the event of a network loop, data packets will pass through the root port.

- **Max Age(Sec)** Read-only object indicates the maximum age of STP information learned from the network (on any port) before it is discarded.

- **Forward Delay(sec)** Read-only object indicates how fast any port on the bridge can change its spanning state when moving towards the forwarding state. The value determines how long the port stays in each of the listening and learning states, which precede the forwarding state.

- **Hold Time(Sec)** Read-only object displays the time interval during which no more than two configuration BPDUs shall be transmitted by the bridge.

- **Root Priority** Read-only object displays the priority number of the root bridge of the Spanning Tree. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multibridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. A bridge priority ranges from 0 to 65535, with 0 being the highest priority.

- **Max Age(6-40 Sec)** Maximum Age is a read-write object that can be set from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root ridge, your Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

- **Hello Time(1-10 Sec)** Hello Time is a read-write object that 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. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

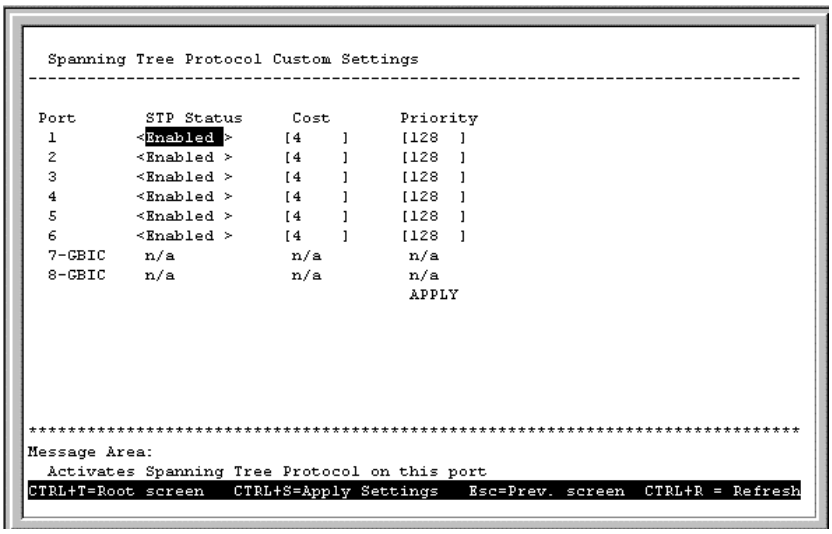
- **Forward Delay(4-30 Sec)** The Forward Delay is a read-write object that can be set from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

- **Bridge Priority(0-65535 Sec)** A Bridge Priority is a read-write object that can be set from 0 to 65535. This is the priority number of the bridge. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multibridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. Zero is the highest priority.

To change the parameters on individual ports:

1. Choose **Configure Spanning Tree Protocol** from the **System Configuration** menu.

2. Choose **STP Port Control** from the **Configure Spanning Tree Protocol** menu. The following screen appears:



```
  Spanning Tree Protocol Custom Settings
-------------------------------------------------------------------------------

 Port       STP Status     Cost       Priority
  1        <Enabled >     [4    ]     [128  ]
  2        <Enabled >     [4    ]     [128  ]
  3        <Enabled >     [4    ]     [128  ]
  4        <Enabled >     [4    ]     [128  ]
  5        <Enabled >     [4    ]     [128  ]
  6        <Enabled >     [4    ]     [128  ]
  7-GBIC    n/a            n/a         n/a
  8-GBIC    n/a            n/a         n/a
                                       APPLY






*******************************************************************************
Message Area:
  Activates Spanning Tree Protocol on this port
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-18. Spanning Tree Protocol Custom Settings screen**

3. Change the *Disabled* setting of the STP Status field to *Enabled*.

4. Set the path cost for the port between 1 and 65535 in the Cost field.

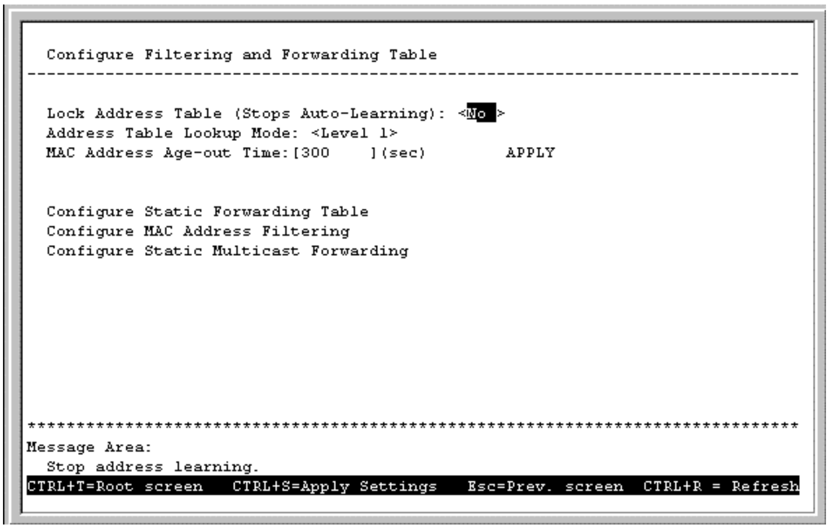
5. Set the priority for the port between 0 and 255 in the Priority field.

6. Press APPLY and hit <Enter>.

## Configure Filtering and Forwarding Table

When a packet hits the Switch, the Switch looks in the filtering and forwarding tables to decide what to do with the packet; either to filter it off the network, or to forward it through the port on which its destination lies. The **Configure Filtering and Forwarding Table** screen allows you to stop or start address learning as well as to select an age-out time of the MAC address in the selected address table. This screen also provides access to three additional configuration screens related to the Switch's filtering and forwarding tables.

Choose **Configure Filtering and Forwarding Table** from the **System Configuration** menu to access the following screen:



```
  Configure Filtering and Forwarding Table
-------------------------------------------------------------------------------

  Lock Address Table (Stops Auto-Learning): <No >
  Address Table Lookup Mode: <Level 1>
  MAC Address Age-out Time:[300    ](sec)         APPLY


  Configure Static Forwarding Table
  Configure MAC Address Filtering
  Configure Static Multicast Forwarding








*******************************************************************************
Message Area:
  Stop address learning.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-19. Configure Filtering and Forwarding Table screen**

The following fields at the top of the screen can be set:

- **Lock Address Table (Stops Auto-Learning)** This function is used mostly for security purposes. When the forwarding table is locked, the Switch will no longer learn the MAC addresses for new hosts. If your network configuration doesn't change, locking the forwarding table helps keep intruders off your network, since any packet coming from an unknown source address will be dropped by the Switch.

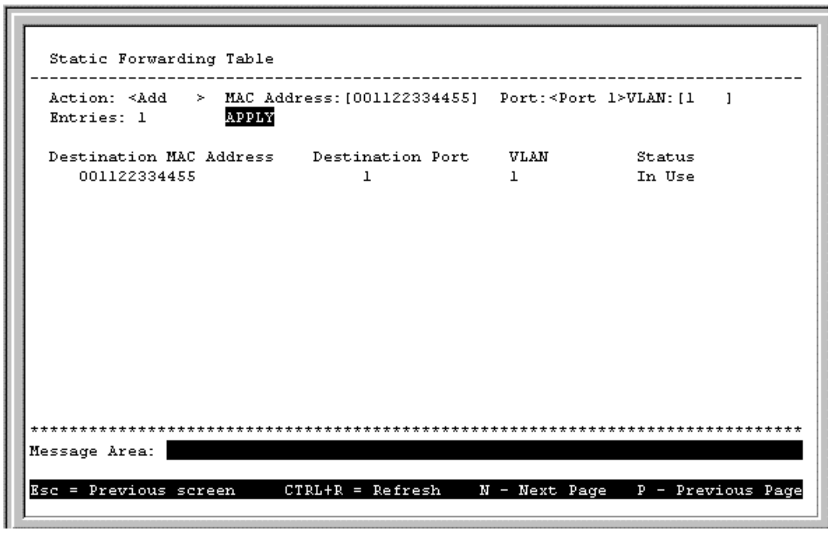
- **Address Table Lookup Mode** This setting allows the user to tailor the MAC address look up procedure. Choices are *Level 0*, *Level 1*, *Level 2*, *Level 3*, *Level 4*, *Level 5*, *Level*, *6*, and *Level 7*. The higher the level, the more MAC addresses can be learned by the Switch. However, a side effect is that throughput will be degraded the higher the level you select. This setting will take effect after your system reboots.

- **MAC Address Age-out Time** Enter the desired MAC address age-out time in this field (10 to 1000000 seconds) .

### *Configure Static Forwarding Table*

The **Static Forwarding Table** screen displays a list of manually defined static MAC address entries.

To access the **Static Forwarding Table** screen, choose **Configure Filtering and Forwarding Table** from the **System Configuration** menu. Then select **Configure Static Forwarding Table** from the bottom of the **Configure Filtering and Forwarding Table** screen. The following screen appears:



```
  Static Forwarding Table
--------------------------------------------------------------------------------
  Action: <Add    >  MAC Address:[001122334455]  Port:<Port 1>VLAN:[1    ]
  Entries: 1         APPLY

  Destination MAC Address    Destination Port    VLAN         Status
     001122334455                  1             1            In Use











********************************************************************************
Message Area:

Esc = Previous screen     CTRL+R = Refresh    N - Next Page   P - Previous Page
```

Figure 6-20.  Static Forwarding Table screen

By mapping a port to a destination MAC address, the Switch can permanently forward traffic to the specified device, even after long periods of network inactivity or during times of network congestion.

To make a change to the **Static Forwarding Table** screen, choose either *Add* or *Remove* in the Action field. Then enter the MAC Address, the Port number that permanently forwards traffic from the specified device, regardless of the device's network activity or current network congestion, enter a VLAN (if applicable), and press APPLY.

The following fields at the top of the screen can be set:

- **Action** Choose *Add* or *Remove* for each entry from the table.

- **MAC Address** Enter a MAC address in this field at the top of the screen. This is the MAC address of the device that you are creating a permanent forwarding address for. A total of ten destination addresses per page will be seen at the bottom of the screen. The Switch can hold up to 256 entries.

- **Port** The port number is entered in this field at the top of the screen. The Switch will always forward traffic to the specified device through this port. The bottom of the screen will display a corresponding destination address.

- **VLAN** Enter the desired VLAN ID number.

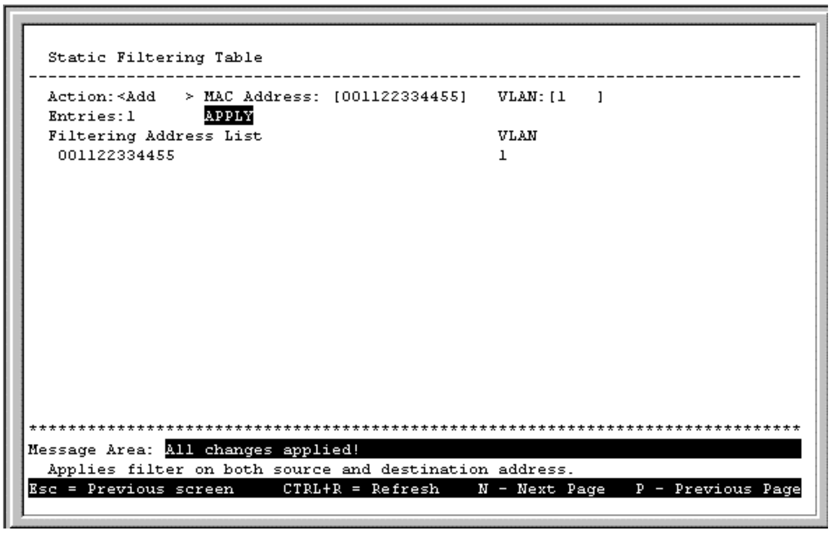
In the lower part of the screen, Destination MAC Address, Destination Port, VLAN, and Status are all read-only fields. The status of the static forwarding table entry can be "in use" or "not apply." "Not apply" means that there is a static filter for the same MAC address. Static filters always take precedence over static forwarding entries. The Switch will automatically upgrade the Status to "in use" once the static filter is removed.

### *Configure MAC Address Filtering*

The **Static Filtering Table** screen contains filtering information configured into the Switch by (local or network) management specifying the set of ports to which packets received from specific ports and containing specific destination addresses are not allowed to be forwarded. You can use the **Static Filtering Table** screen for network security purposes thereby discarding unwanted addresses from the Forwarding Table.

Dynamic Filtering and Static Filtering are among the two important features of the **Static Filtering Table**. They are defined here briefly as follows. *Dynamic Filtering* is when a dynamic entry is created by the Learning Process as a result of observation of network traffic in the Filtering Database. *Static Filtering* is defined as static entries that may be added and removed from the Filtering Database by the user. They are not automatically removed by any timeout mechanism.

To access the **Static Filtering Table** screen, select **Configure Filtering and Forwarding Table** from the **System Configuration** menu. Then select **Configure MAC Address Filtering** from the bottom of the **Configure Filtering and Forwarding Table** screen. The following screen appears:



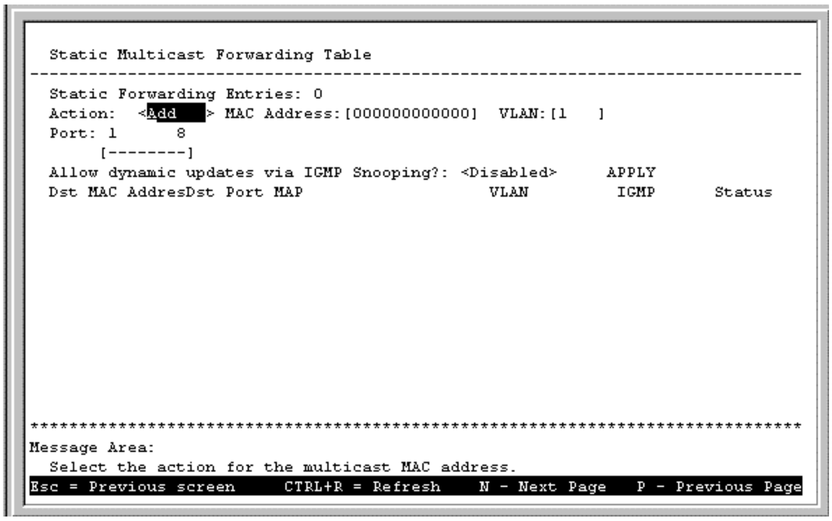
```
  Static Filtering Table
-------------------------------------------------------------------------------
  Action:<Add    > MAC Address: [001122334455]   VLAN:[1    ]
  Entries:1        APPLY
  Filtering Address List                         VLAN
   001122334455                                  1















*******************************************************************************
Message Area: All changes applied!
  Applies filter on both source and destination address.
Esc = Previous screen     CTRL+R = Refresh    N - Next Page   P - Previous Page
```

Figure 6-21. Static Filtering Table screen

To make a change to the **Static Filtering Table** screen, choose *Add* or *Remove* in the Action field. Then enter the MAC Address and VLAN ID number (if applicable) and press APPLY.

### *Configure Static Multicast Forwarding*

The **Static Multicast Forwarding Table** screen allows you to forward traffic over each port for one multicast group. To access this screen, select **Configure Static Multicast Forwarding** from the **Configure Filtering and Forwarding Table** screen. The following screen will appear:



```
  Static Multicast Forwarding Table
-------------------------------------------------------------------------------
  Static Forwarding Entries: 0
  Action:  <Add     > MAC Address:[000000000000]  VLAN:[1    ]
  Port: 1      8
       [--------]
  Allow dynamic updates via IGMP Snooping?: <Disabled>     APPLY
  Dst MAC AddresDst Port MAP                   VLAN         IGMP      Status












*******************************************************************************
Message Area:
  Select the action for the multicast MAC address.
Esc = Previous screen     CTRL+R = Refresh    N - Next Page   P - Previous Page
```

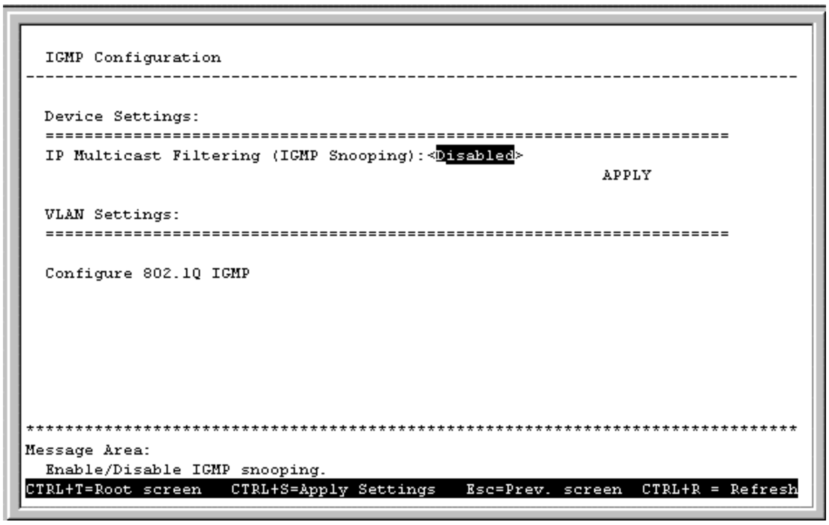
Figure 6-22. Static Multicast Forwarding Table screen

To make a change to the **Static Multicast Forwarding Table** screen above, choose *Add* or *Remove* in the Action field. Then enter the MAC Address and VLAN. Next place a *V* over the dash "–" in the Port field to assign outgoing ports. You may also use this screen to allow dynamic updates via IGMP snooping by toggling the last field to *Enabled*. Press APPLY to put the changes into effect.

## Configure IGMP Filtering

Internet Group Management Protocol (IGMP) allows multicasting on your network. When IP Multicast Filtering is enabled, the Switch can intelligently forward (rather that broadcast) IGMP queries and reports sent between devices connected to the Switch and an IGMP-enabled device hosting IGMP on your network. 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.

To access the **IGMP Configuration** screen, select **Configure IGMP Filtering** from the **System Configuration** menu. The following **IGMP Configuration** screen will appear:



```
  IGMP Configuration
-------------------------------------------------------------------------------

  Device Settings:
  ======================================================================
  IP Multicast Filtering (IGMP Snooping):<Disabled>
                                                        APPLY

  VLAN Settings:
  ======================================================================

  Configure 802.1Q IGMP






*******************************************************************************
Message Area:
  Enable/Disable IGMP snooping.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

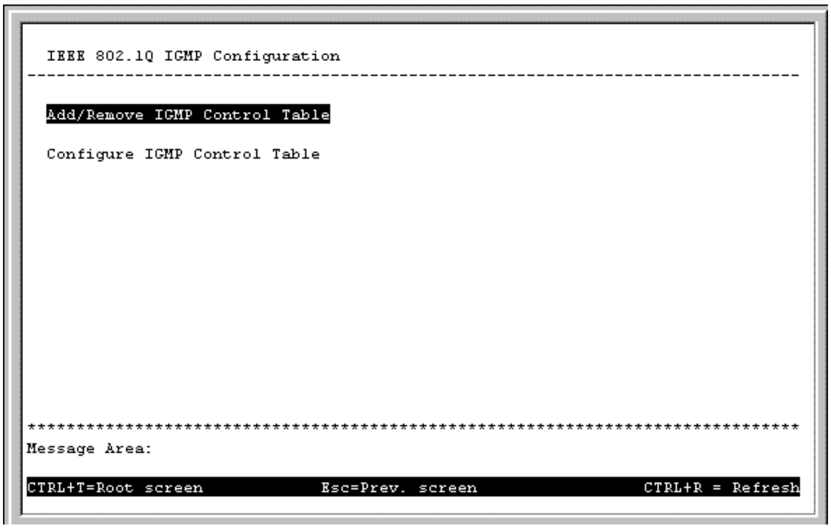
**Figure 6-23. IGMP Configuration screen**

The item in this screen is defined as follows:

♦ **IP Multicast Filtering (IGMP Snooping)** This enables or disables the Switch to intelligently forward IGMP and Multicast packets instead of broadcasting (flooding) them on all ports. This setting also enables IGMP Snooping, which enables the switch to read IGMP packets being forwarded through the switch in order to obtain forwarding information from them (learn which ports contain Multicast members).

### *Configure 802.1Q IGMP*

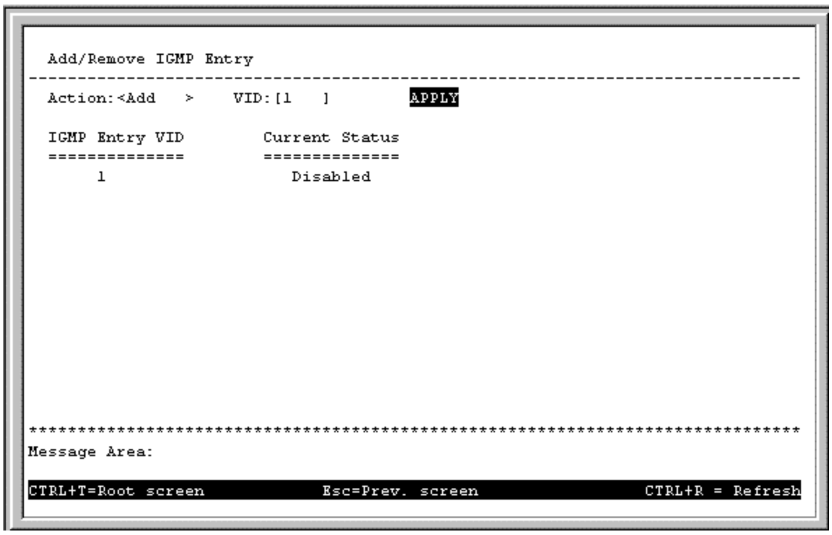
If the Switch is in IEEE 802.1Q VLANs mode, the **IGMP Configuration** screen will offer a VLAN Settings section in the lower part of the screen. Select Configure 802.1Q IGMP to access the following **IEEE 802.1Q IGMP Configuration** menu:



```
 IEEE 802.1Q IGMP Configuration
--------------------------------------------------------------------------------

 Add/Remove IGMP Control Table

 Configure IGMP Control Table















********************************************************************************
Message Area:

CTRL+T=Root screen           Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-24. IEEE 802.1Q IGMP Configuration menu

Choose **Add/Remove IGMP Control Table** from the screen above to define up to 12 VLANs on the Switch which can send and receive IGMP packets:



```
 Add/Remove IGMP Entry
--------------------------------------------------------------------------------
 Action:<Add   >    VID:[1    ]        APPLY

 IGMP Entry VID        Current Status
 ==============        ==============
      1                   Disabled












********************************************************************************
Message Area:

CTRL+T=Root screen           Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-25. Add/Remove IGMP Entry screen

The above screen is used to specify an agent to interface between IGMP and VLAN. The agents are assigned to a VLAN and allow IGMP query and report packets to be present on the given VLAN. Only 12 agents can exist on the switch at any one time.

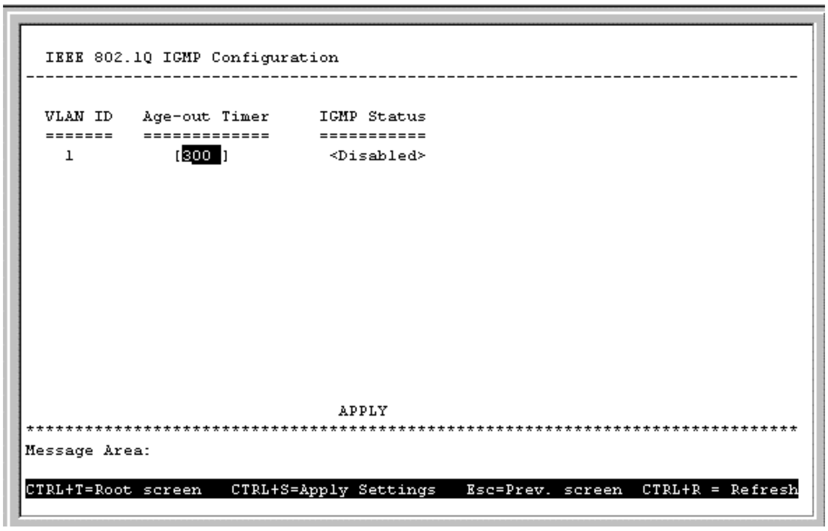
Items in the above screen are described below:

♦ **Action** Adds or removes an entry (agent) from the table.

♦ **VID** The VLAN number that you wish to create an agent for.

Press APPLY to add the agent to the table.

Go back to the **IEEE 802.1Q IGMP Configuration** menu and choose **Configure IGMP Control Table** in order to activate or deactivate the agents and configure settings for them. The following **IEEE 802.1Q IGMP Configuration** screen appears:



```
 IEEE 802.1Q IGMP Configuration
-------------------------------------------------------------------------------

 VLAN ID   Age-out Timer     IGMP Status
 =======   =============     ===========
   1          [300 ]          <Disabled>














                                APPLY
*******************************************************************************
Message Area:

CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-26.  IEEE 802.1Q IGMP Configuration screen

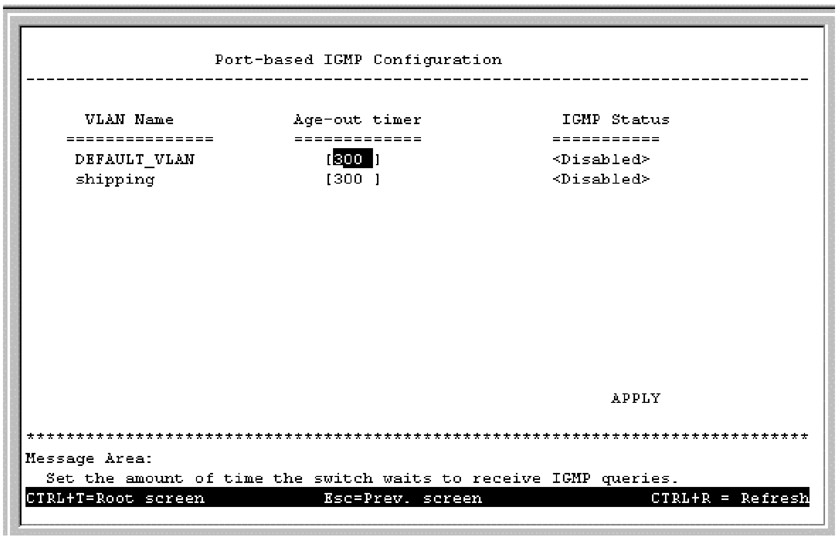
This allows you to enable or disable these agents and set aging timers for them.

Items in the above screen are defined as follows:

- **VLAN ID**  This is the VID number for the VLAN that has an agent attached to it which enables IGMP packets to be sent and received.
- **Age-out Timer**  If no IGMP query packet has arrived at the Switch before this timer has expired, the Switch will become the IGMP host for this VLAN.
- **IGMP Status**  Activates or deactivates the agent on this VLAN.

### *Configure Port-based IGMP*

If the Switch is in Port-based mode, the **IGMP Configuration** screen will offer a VLAN Settings section in the lower part of the screen. Select Configure Port-based IGMP to access the following **Port-based IGMP Configuration** screen:



```
                  Port-based IGMP Configuration
-------------------------------------------------------------------------------

      VLAN Name           Age-out timer            IGMP Status
    ===============       =============           ===========
     DEFAULT_VLAN            [300 ]               <Disabled>
     shipping                [300 ]               <Disabled>












                                                          APPLY

*******************************************************************************
Message Area:
  Set the amount of time the switch waits to receive IGMP queries.
CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

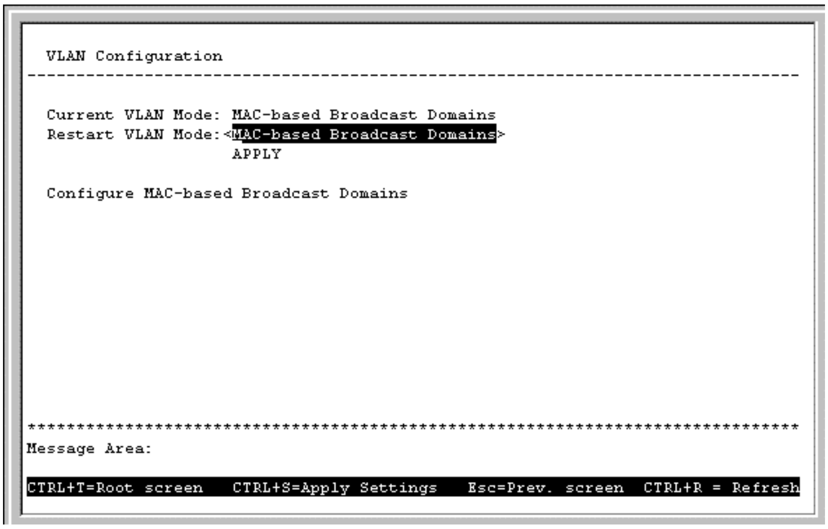
Figure 6-27.  Port-based IGMP Configuration screen

After you have set the age-out timer and either enabled or disabled IGMP status for the desired VLAN, press APPLY to let the changes take effect.

## Configure VLAN

The **VLAN Configuration** menu displays the status of the current VLAN mode and allows a user to restart the Switch in *IEEE 802.1Q VLANs*, *Port-based*, or *MAC-based Broadcast Domains* mode, or not to use a selection by choosing *None*. Please note that the Switch can only support one mode at any given time. Also, each time the mode is changed, the Switch must be rebooted before the new mode is activated.

If you have selected *MAC-based Broadcast Domains* and then rebooted the Switch, **Configure MAC-based Broadcast Domains** will appear at the bottom of the **VLAN Configuration** screen (**System Configuration → Configure VLANs**):



```
  VLAN Configuration
-------------------------------------------------------------------------------

  Current VLAN Mode: MAC-based Broadcast Domains
  Restart VLAN Mode:<MAC-based Broadcast Domains>
                     APPLY

  Configure MAC-based Broadcast Domains

*******************************************************************************
Message Area:

CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-28. VLAN Configuration screen**

The information on the top of the screen is described as follows:

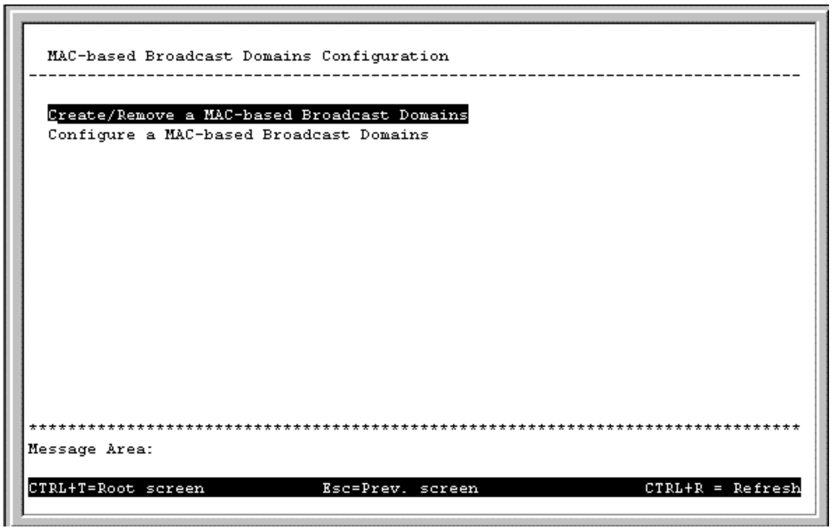
- **Current VLAN Mode** Displays what mode, if any, is currently enabled on the Switch.
- **Restart VLAN Mode** Choose from four settings for this mode: *MAC-based Broadcast Domains, IEEE 802.1Q VLANs, Port-based,* or *None*. After being restarted, the Switch will implement the setting you have chosen.

### *Configure MAC-based Broadcast Domains*

To create MAC-based broadcast domains**,** simply create the broadcast domain itself in the **Add/Remove MAC-based Broadcast Domains** screen, and then enter MAC addresses to the broadcast domain in the **Add/Remove MAC-based Broadcast Domain Members** screen. Afterwards, restart the Switch and the broadcast domain will be implemented.

Please note that if the mode is set to *MAC-based Broadcast Domains*, then the Port Lock function is not supported in the **Port Configuration** screen and the Lock Address Table function located on the **Configure Filtering and Forwarding Table** screen is not available.

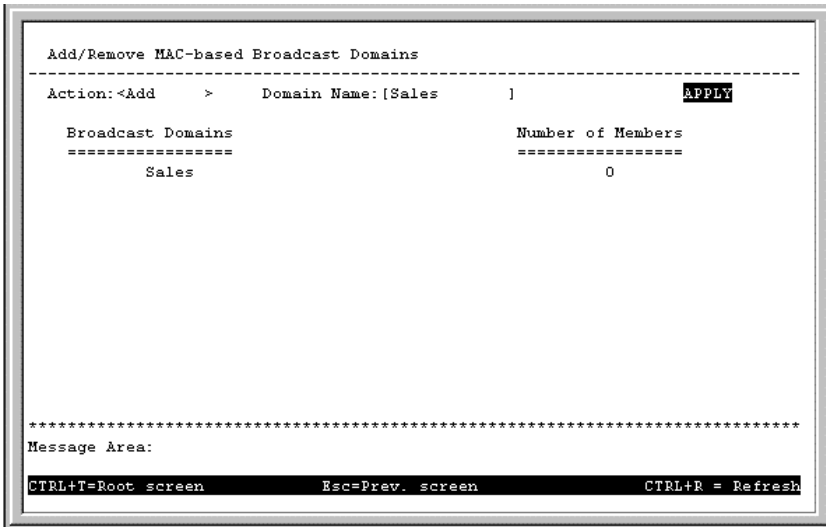
Choose **Configure MAC-based Broadcast Domains** from the bottom of the **VLAN Configuration** screen above to access the **MAC-Based Broadcast Domains Configuration** menu:



```
 MAC-based Broadcast Domains Configuration
-------------------------------------------------------------------------------

 Create/Remove a MAC-based Broadcast Domains
 Configure a MAC-based Broadcast Domains

*******************************************************************************
Message Area:

CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-29. MAC-based Broadcast Domains Configuration menu

Choose **Add/Remove MAC-based Broadcast Domains** to access the following screen:



```
 Add/Remove MAC-based Broadcast Domains
-------------------------------------------------------------------------------
 Action:<Add     >     Domain Name:[Sales        ]                APPLY

   Broadcast Domains                             Number of Members
   =================                             =================
           Sales                                          0

*******************************************************************************
Message Area:

CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-30. Add/Remove MAC-based Broadcast Domains screen

The fields you can set are:

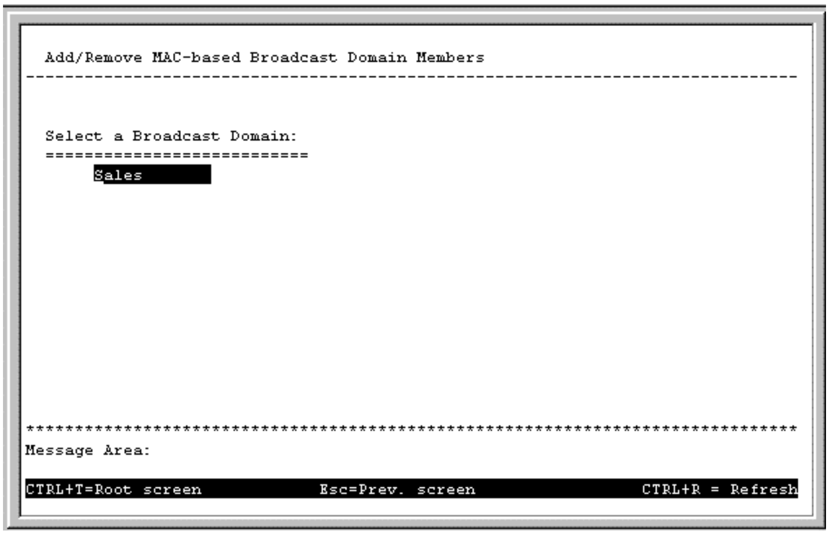
♦ **Action** Select the desired action by toggling between *Add* and *Remove.*

♦ **Domain Name** Enter the name of the broadcast domain.

Press APPLY to add or remove the designated MAC-based broadcast domain.

Broadcast Domains and Number of Members reflect the current status. They are read-only fields and cannot be changed.

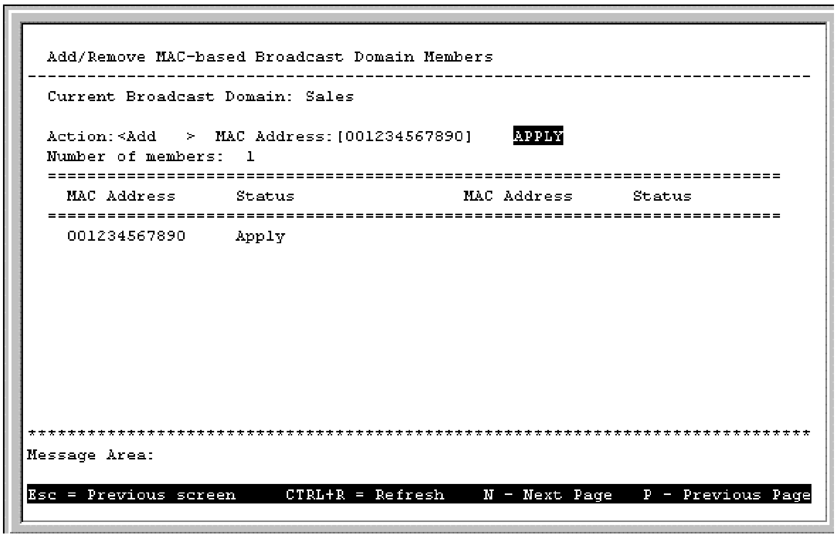
Choose **Add/Remove MAC-based Broadcast Domain Members** from the **MAC-Based Broadcast Domains Configuration** menu to access the following screen:



```
 Add/Remove MAC-based Broadcast Domain Members
--------------------------------------------------------------------------------


 Select a Broadcast Domain:
 ===========================
      Sales












********************************************************************************
Message Area:

CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-31.  First Add/Remove MAC-based Broadcast Domain Members screen

To configure a broadcast domain, highlight the desired entry on the screen above and press <Enter>. The following **Add/Remove MAC-based Broadcast Domain Members** screen appears:



```
 Add/Remove MAC-based Broadcast Domain Members
--------------------------------------------------------------------------------
 Current Broadcast Domain: Sales

 Action:<Add   >  MAC Address:[001234567890]     APPLY
 Number of members:  1
 ===========================================================================
   MAC Address      Status                 MAC Address      Status
 ===========================================================================
   001234567890     Apply










********************************************************************************
Message Area:

Esc = Previous screen      CTRL+R = Refresh    N - Next Page   P - Previous Page
```

Figure 6-32.  Second Add/Remove MAC-based Broadcast Domain Members screen

The fields you can set are:

♦ **Action**  Select the desired action by toggling between *Add* and *Remove.*

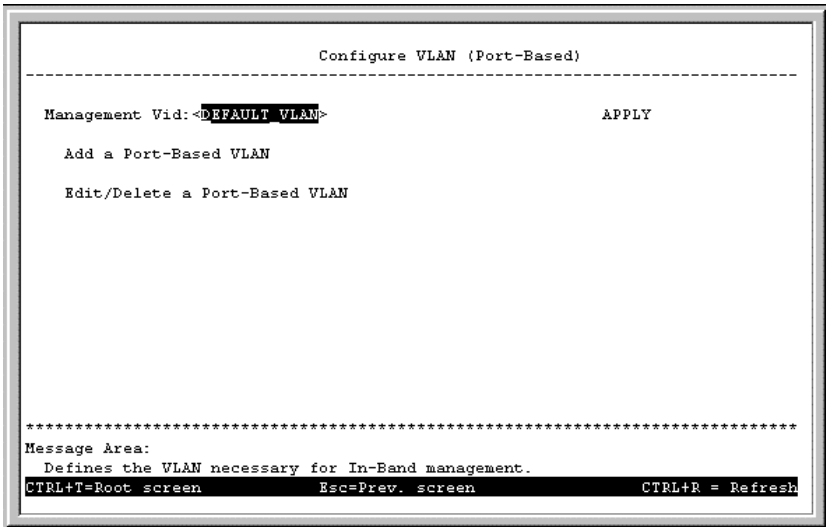
♦ **MAC Address**  The MAC address of the broadcast domain member being added or removed.

Please note that the Status field for the MAC address you have entered may read *Not-Apply*. Once the Switch is restarted in MAC-based broadcast domain mode, the MAC-addresses will be applied, meaning that the broadcast domain is active.

Current Broadcast Domain, Number of members, MAC Address (in the lower part of the screen), and Status reflect the current conditions. They are read-only fields and cannot be changed.

### Configure Port-based VLANs

Choose **Configure Port-based VLANs** on the **VLAN Configuration** screen (**System Configuration → Configure VLANs & MAC-based Broadcast Domains**) to access the **Port-based VLAN Configuration** menu pictured below (note that if you have just changed to this mode, you must also reboot the Switch before being able to work with port-based VLANs):



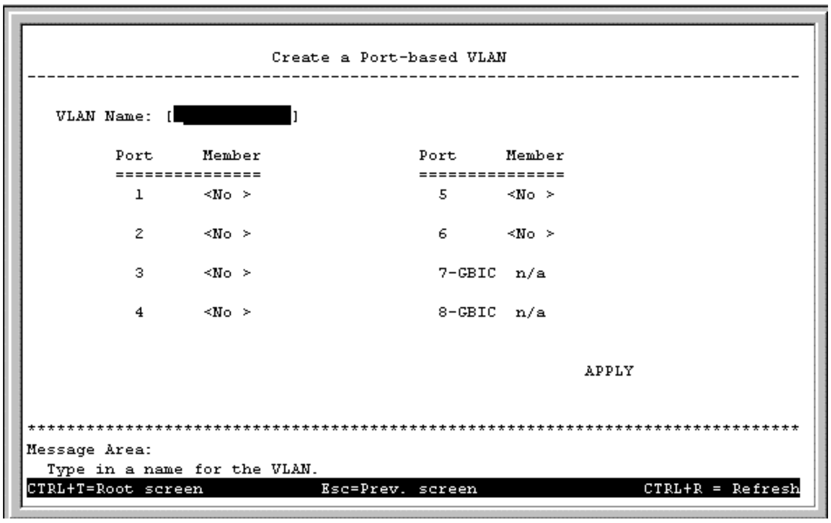
```
                              Configure VLAN (Port-Based)
-------------------------------------------------------------------------------

  Management Vid:<DEFAULT_VLAN>                                   APPLY

    Add a Port-Based VLAN

    Edit/Delete a Port-Based VLAN










*******************************************************************************
Message Area:
  Defines the VLAN necessary for In-Band management.
CTRL+T=Root screen            Esc=Prev. screen                CTRL+R = Refresh
```

Figure 6-33. Configure VLAN (Port-Based) menu

The field you can set is:

♦ **Management Vid** Enter a VLAN name for use with in-band management.

Select **Add a Port-Based VLAN** from the menu above to access the following screen:

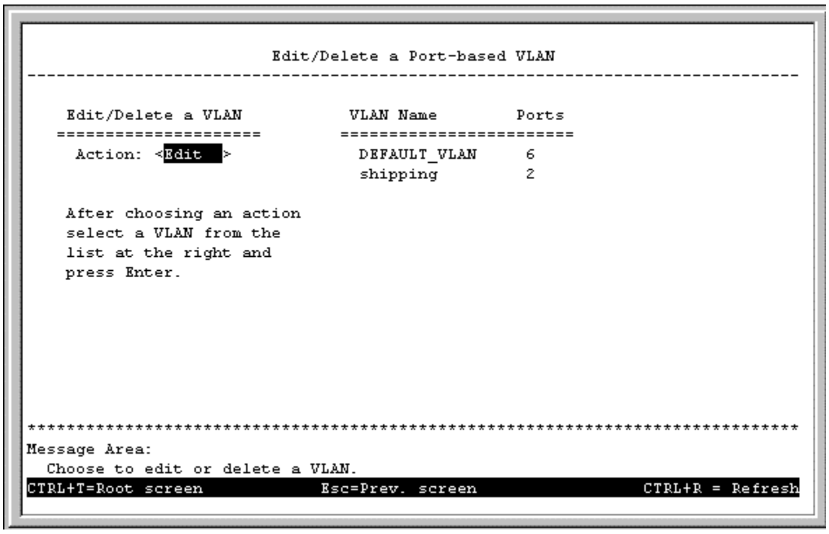


```
                         Create a Port-based VLAN
-------------------------------------------------------------------------------

   VLAN Name: [            ]

         Port     Member                Port     Member
         ===============                ===============
           1      <No >                   5      <No >

           2      <No >                   6      <No >

           3      <No >                   7-GBIC  n/a

           4      <No >                   8-GBIC  n/a


                                                                APPLY

*******************************************************************************
Message Area:
  Type in a name for the VLAN.
CTRL+T=Root screen            Esc=Prev. screen                CTRL+R = Refresh
```

Figure 6-34. Create a Port-based VLAN screen

To create a port-based VLAN, fill in the VLAN Name field in the screen above. Next toggle *Yes* or *No* for each port member. Press APPLY to let the changes take effect.

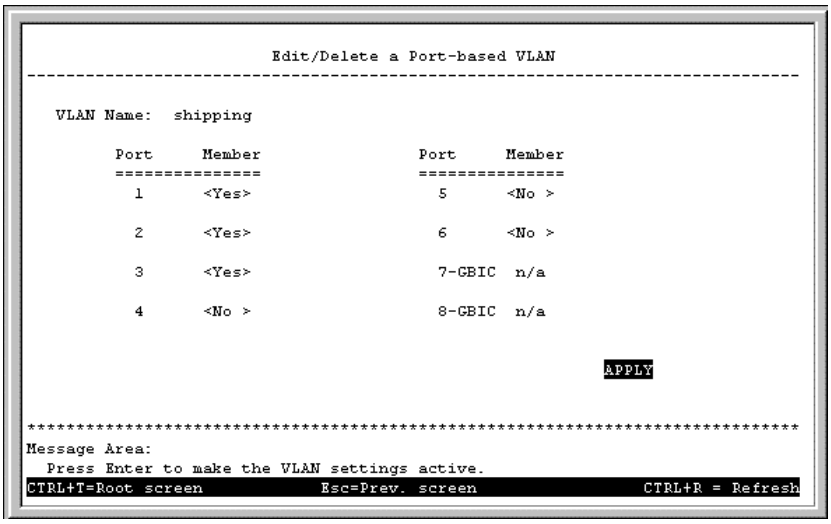
To edit or delete a port-based VLAN, select **Edit/Delete a Port-Based VLAN** from the **Configure VLAN (Port-Based)** screen. The following screen appears:



```
                          Edit/Delete a Port-based VLAN
-------------------------------------------------------------------------------

    Edit/Delete a VLAN          VLAN Name        Ports
   =====================       ========================
     Action: <Edit   >           DEFAULT_VLAN     6
                                 shipping         2

    After choosing an action
    select a VLAN from the
    list at the right and
    press Enter.

*******************************************************************************
Message Area:
  Choose to edit or delete a VLAN.
CTRL+T=Root screen           Esc=Prev. screen                CTRL+R = Refresh
```

Figure 6-35. first Edit/Delete a Port-based VLAN screen

Select *Edit* or *Delete* in the Action field and then select a VLAN from the column on the right side of the screen above. The following screen appears:



```
                          Edit/Delete a Port-based VLAN
-------------------------------------------------------------------------------

   VLAN Name:  shipping

         Port     Member                Port     Member
         ===============                ===============
           1      <Yes>                   5      <No >

           2      <Yes>                   6      <No >

           3      <Yes>                   7-GBIC  n/a

           4      <No >                   8-GBIC  n/a

                                                             APPLY

*******************************************************************************
Message Area:
  Press Enter to make the VLAN settings active.
CTRL+T=Root screen           Esc=Prev. screen                CTRL+R = Refresh
```

Figure 6-36. second Edit/Delete a Port-based VLAN screen

Toggle between *Yes* or *No* to assign a port to be a member of the selected VLAN. Press APPLY to let the changes take effect.

### *Configure 802.1Q VLAN*

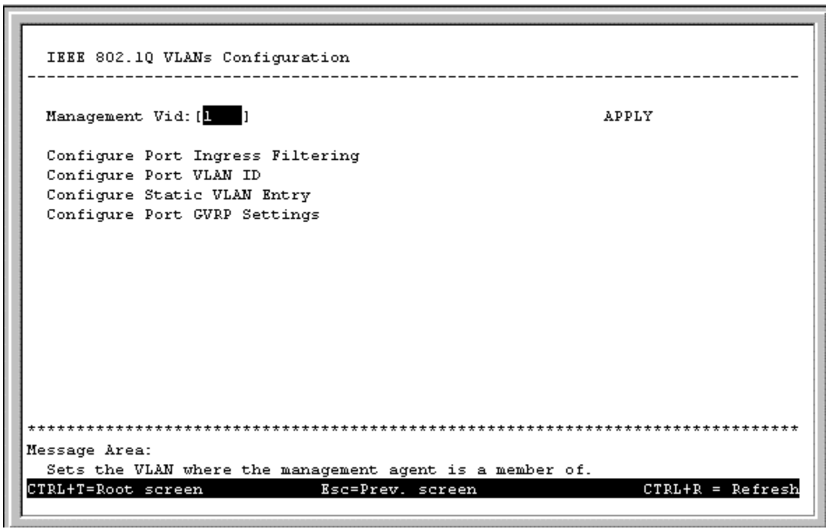
To configure an IEEE 802.1Q VLAN, you must do three things:

1. Decide if you want to enable Ingress Filtering and enable it on the chosen ports. Ingress filtering applied on a port causes the port to examine all incoming packets and check whether the port itself is a member of the VLAN. This is normally used to keep untagged frames off the Switch, although it can have other uses as well. This setting is configurable for each port in the **Ingress Filtering** screen.

2. Define which ports will be active members of the VLAN. A port can transmit packets onto only one VLAN. It can receive packets (be a passive member) on many VLANs. Active VLANs are designations defined by assigning Port VLAN ID numbers (PVIDs) in the **Port VLAN assignment** screen.

3. Define the VLAN itself and which ports will be members (able to receive packets from a port that has this PVID number). At this point, you need to designate whether a member port will be a Tagging or Untagging member port. Defining the ports that will be members of a VLAN, and whether they will Tag or Untag packets is done in the **802.1Q Static VLAN Settings** screen.

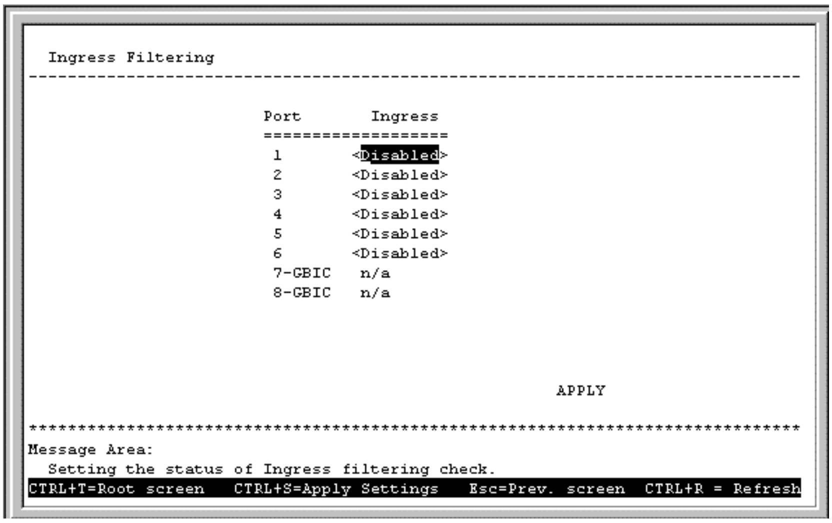
Choose **Configure 802.1Q VLAN** on the **VLAN Configuration** screen (**System Configuration → Configure VLAN**) to access the **IEEE 802.1Q VLANs Configuration** menu pictured below (note that if you have just changed to this mode, you must also reboot the Switch before being able to work with IEEE 802.1Q VLANs):



```
  IEEE 802.1Q VLANs Configuration
-------------------------------------------------------------------------------

  Management Vid: [1   ]                                     APPLY

  Configure Port Ingress Filtering
  Configure Port VLAN ID
  Configure Static VLAN Entry
  Configure Port GVRP Settings

*******************************************************************************
Message Area:
  Sets the VLAN where the management agent is a member of.
CTRL+T=Root screen            Esc=Prev. screen                CTRL+R = Refresh
```

Figure 6-37. IEEE 802.1Q VLANs Configuration screen

Choose **Configure Port Ingress Filtering** to access the first item on the menu. The following screen appears:



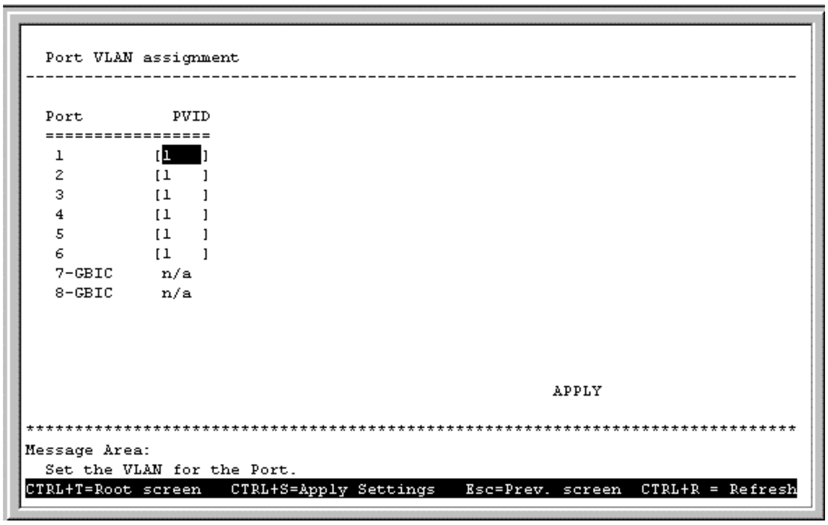
```
  Ingress Filtering
-------------------------------------------------------------------------------

                        Port       Ingress
                        ===================
                         1       <Disabled>
                         2       <Disabled>
                         3       <Disabled>
                         4       <Disabled>
                         5       <Disabled>
                         6       <Disabled>
                         7-GBIC   n/a
                         8-GBIC   n/a

                                                        APPLY

*******************************************************************************
Message Area:
  Setting the status of Ingress filtering check.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-38. Ingress Filtering screen

This screen allows you to set Ingress filtering for each port to either *Enabled* or *Disabled*. When a packet arrives at the port and Ingress filtering is *Enabled*, the port will check the VLAN ID number of the packet, and its own VIDs. If there is a match, the port will receive the packet. If the packet doesn't have a VLAN tag or the port is not a member of the VLAN for which the packet is tagged, the packet will be discarded.

***Note:*** If a port is a member of a trunk group but is not the anchor, the items shown in the above table will be read-only and the values will be the same as those for the anchor port.

Choose **Configure Port VLAN ID** to access the second item on the **IEEE 802.1Q VLAN Configuration** menu. The following screen appears:



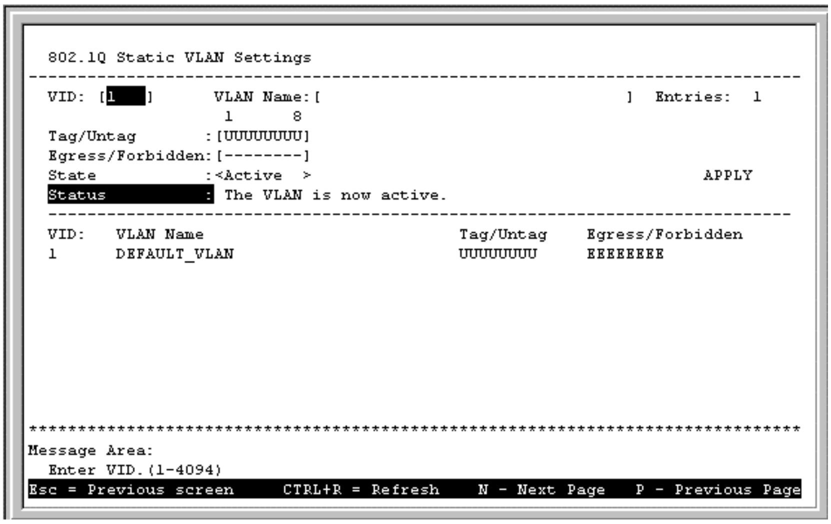
```
  Port VLAN assignment
-------------------------------------------------------------------------------

  Port        PVID
  ================
   1         [1   ]
   2         [1   ]
   3         [1   ]
   4         [1   ]
   5         [1   ]
   6         [1   ]
   7-GBIC     n/a
   8-GBIC     n/a

                                                      APPLY

*******************************************************************************
Message Area:
  Set the VLAN for the Port.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-39. Port VLAN assignment screen**

This screen allows you to set a default port VLAN ID number (PVID) for each port. Press APPLY to let the changes take effect.

***Note:*** If a port is a member of a trunk group but is not the anchor, the items shown in the above table will be read-only and the values will be the same as those for the anchor port.

Choose **Configure Static VLAN Entry** to access the third item on the **IEEE 802.1Q VLANs Configuration** menu. The following screen appears:



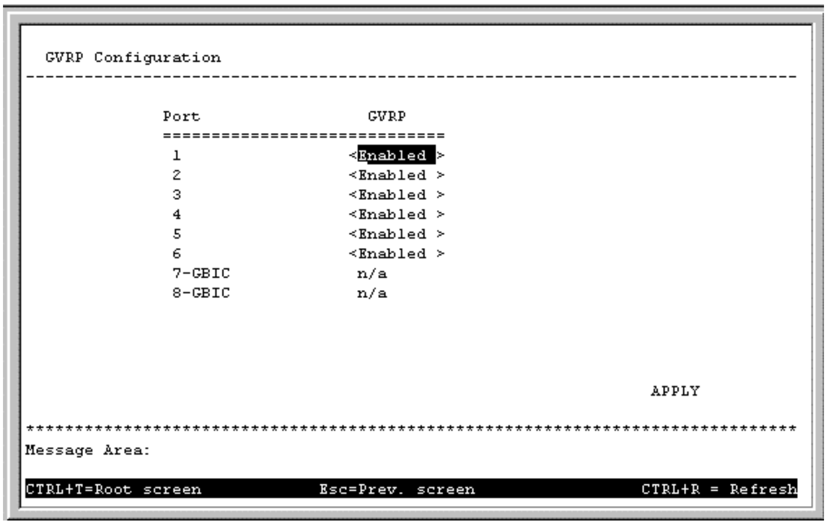
```
  802.1Q Static VLAN Settings
-------------------------------------------------------------------------------
  VID: [1   ]     VLAN Name:[                              ]  Entries:  1
                         1      8
  Tag/Untag         :[UUUUUUUU]
  Egress/Forbidden:[--------]
  State             :<Active  >                                    APPLY
  Status            : The VLAN is now active.
  -----------------------------------------------------------------------------
  VID:   VLAN Name                         Tag/Untag    Egress/Forbidden
  1      DEFAULT_VLAN                      UUUUUUUU     EEEEEEEE

*******************************************************************************
Message Area:
  Enter VID.(1-4094)
Esc = Previous screen     CTRL+R = Refresh    N - Next Page   P - Previous Page
```

**Figure 6-40. 802.1Q Static VLAN Settings screen**

The fields above include:

- **VID** Enter a VLAN ID from 1 to 4094 and hit <Enter>. This is the VLAN that will be defined on this screen.
- **VLAN Name** Description of the VLAN.
- **Tag/Untag** Toggle between *T* for tag and *U* for untag for each port.
- **Egress/Forbidden** Position the cursor over the dash "–" representing the appropriate port number and press <space bar> to select *E* for Egress membership, or leave the dash "– ". An *E* designates the specified port as a static member of the VLAN. A dash means the port is not given VLAN membership for the VID entered above.
- **State** Toggle between *Active* and *Inactive.*
- **Status** This indicates the current 802.1Q Static VLAN status.

Choose **Configure Port GVRP Settings** to access the fourth item on the **IEEE 802.1Q VLANs Configuration** menu. The following screen appears:



```
 GVRP Configuration
------------------------------------------------------------------------------

             Port                 GVRP
             ============================
              1                 <Enabled >
              2                 <Enabled >
              3                 <Enabled >
              4                 <Enabled >
              5                 <Enabled >
              6                 <Enabled >
              7-GBIC             n/a
              8-GBIC             n/a



                                                             APPLY

******************************************************************************
Message Area:

CTRL+T=Root screen           Esc=Prev. screen              CTRL+R = Refresh
```

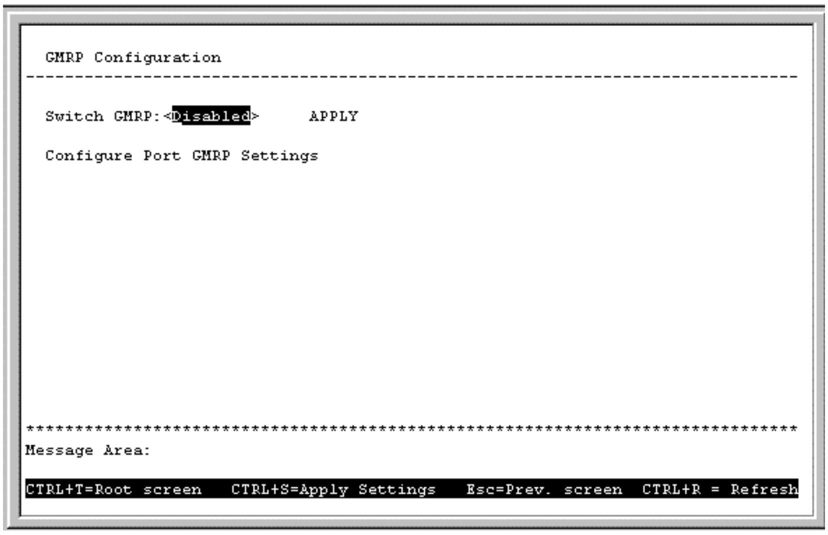
**Figure 6-41. GVRP Configuration screen**

This screen allows you to enable or disable GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol, on individual ports. GVRP updates dynamic VLAN registration entries and communicates the new VLAN information across the network. This allows, among other things, for stations to physically move to other switch ports and keep their same VLAN settings, without having to reconfigure VLAN settings on the Switch. Press APPLY to let your changes take effect.

### *Configure GMRP*

Group Multicast Registration Protocol (GMRP) allows multicasts to be sent on a single VLAN without affecting other VLANs or broadcast domains. Group registration entries indicate for each port whether frames to be sent to a group MAC address and on a certain VLAN should be filtered or discarded. Use the **GMRP Configuration** screen to enable or disable GMRP.

To make GMRP configuration changes, select **Configure GMRP** at the bottom of the **VLAN Configuration** menu (when *IEEE 802.1Q VLANs* is set). The following screen appears:

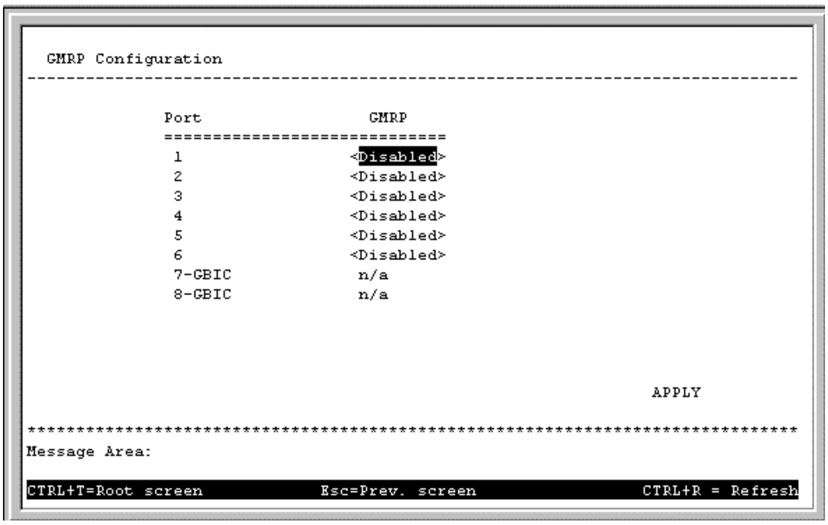


```
 GMRP Configuration
-------------------------------------------------------------------------------

 Switch GMRP:<Disabled>     APPLY

 Configure Port GMRP Settings










*******************************************************************************
Message Area:

CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-42. GMRP Configuration menu

The Switch GMRP field allows you to either enable or disable GMRP on the Switch by toggling between the two choices and then pressing APPLY to let the change take effect.

Once GMRP is enabled for the Switch, you then must enable specific ports by selecting **Configure Port GMRP Settings** from the **GMRP Configuration** menu above. The **GMRP Configuration** screen appears:



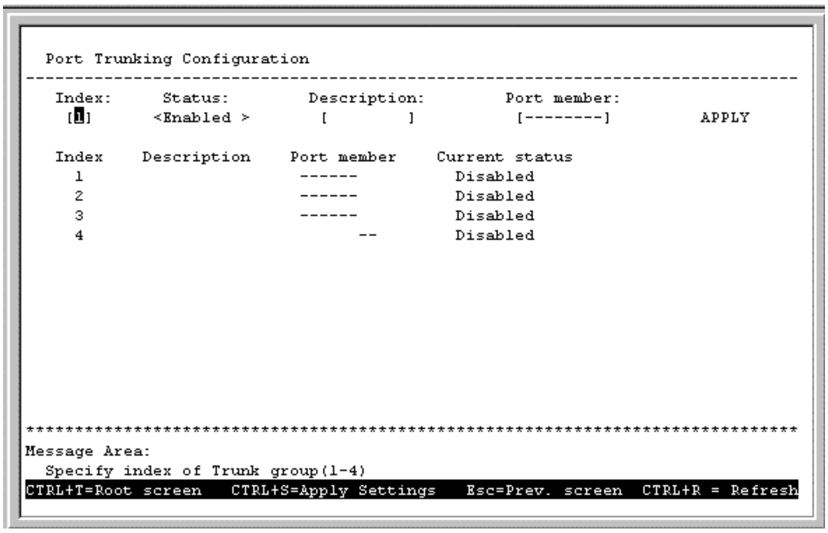
```
 GMRP Configuration
-------------------------------------------------------------------------------

             Port                GMRP
             =============================
              1                <Disabled>
              2                <Disabled>
              3                <Disabled>
              4                <Disabled>
              5                <Disabled>
              6                <Disabled>
              7-GBIC            n/a
              8-GBIC            n/a




                                                              APPLY

*******************************************************************************
Message Area:

CTRL+T=Root screen           Esc=Prev. screen                  CTRL+R = Refresh
```

Figure 6-43. GMRP Configuration screen

Use this screen to enable or disable GMRP on individual ports. Press APPLY to let your changes take effect.

## Configure Trunk

Ports on the switch can be grouped together in a single logical port called a trunk. This is discussed in detail in the *Port Trunking* section of the chapter of this manual entitled "*Switch Management Concepts.*" To set up a trunk group, choose **Configure Trunk** from the **System Configuration** menu. The following screen appears:



```
 Port Trunking Configuration
------------------------------------------------------------------------------
  Index:     Status:        Description:        Port member:
   [1]      <Enabled >       [         ]         [--------]        APPLY

  Index    Description    Port member    Current status
    1                      ------          Disabled
    2                      ------          Disabled
    3                      ------          Disabled
    4                            --        Disabled









******************************************************************************
Message Area:
 Specify index of Trunk group(1-4)
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-44. Port Trunking Configuration screen

Please note that the maximum size for trunk groups 1 to 3 is 4 ports. Trunk group 4 is two ports.

The fields you can set are:

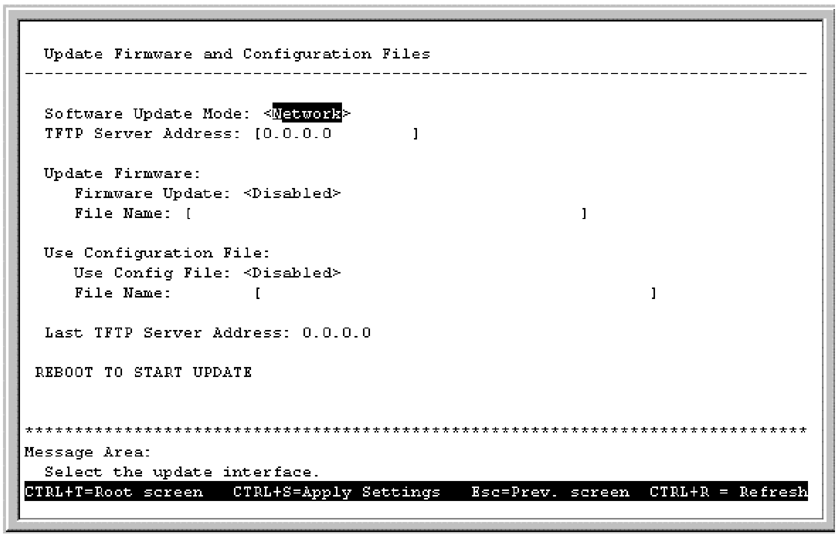
- **Index** Enter the index number (1 through 4, as shown in this screen) that you wish to give the new entry, or the index number of the entry that you wish to remove.
- **Status** Use the space bar to toggle between *Enabled* and *Disabled*. This indicates whether you want to add or remove a trunk group. Be careful when removing trunk groups as the connections will return to normal operation, which may cause signal loops.
- **Description** Enter the desired group name. This can be any text string.
- **Port Member** Select two or more ports for this field. Use the arrow keys to move the cursor, and the *V* and hyphen keys to select and deselect ports.

Press APPLY to make the changes take effect. The new settings will appear in the table at the bottom of this screen.

## Update Firmware and Configuration Files

The Switch is capable of obtaining its boot-time configuration information, as well as updated versions of its internal firmware, using TFTP (the Trivial File Transfer Protocol) and BOOTP (the BOOTstrap Protocol). You can use the **Update Firmware and Configuration Files** screen to control this feature.

Choose **Update Firmware and Configuration Files** on the Switch's main menu. The following screen appears:



```
 Update Firmware and Configuration Files
--------------------------------------------------------------------------------

 Software Update Mode: <Network>
 TFTP Server Address: [0.0.0.0        ]

 Update Firmware:
    Firmware Update: <Disabled>
    File Name: [                                    ]

 Use Configuration File:
    Use Config File: <Disabled>
    File Name:        [                                    ]

 Last TFTP Server Address: 0.0.0.0

REBOOT TO START UPDATE


********************************************************************************
Message Area:
 Select the update interface.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-45. Update Firmware and Configuration Files screen**

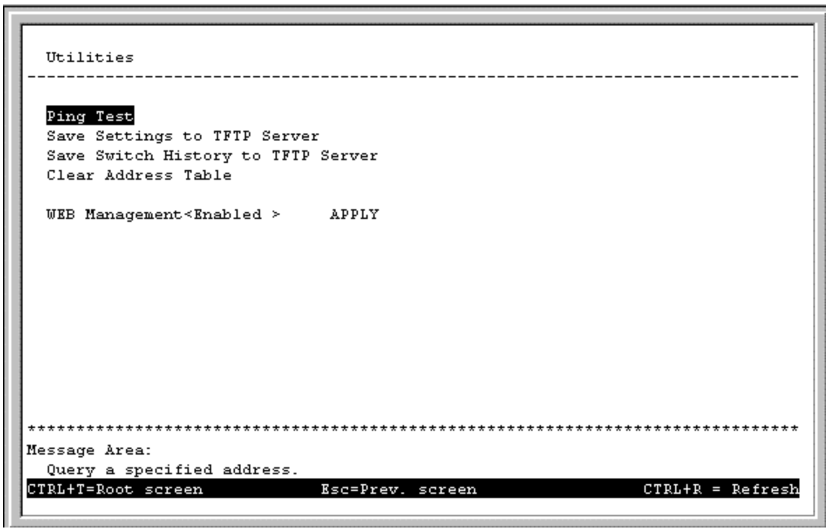
The fields you can set are:

- **Software Update Mode** Set to either *Network* or *SLIP*. Determines whether the configuration file should be obtained through the Ethernet network or through the console port.
- **TFTP Server Address** The IP address of the TFTP server where the configuration file is located. This entry is used only if the Firmware Update is set to *Enabled*. If BOOTP Service (see the IP Configuration screen under Configure IP Address on the System Configuration menu) is set to *Enabled*, the address will be obtained from the BOOTP server.
- **Firmware Update** Determines whether or not the Switch will try to look for a runtime image file over the network. If set to *Disabled*, none of the fields below have any effect.
- **File Name** The pathname of the runtime image file on your TFTP server to be downloaded.
- **Use Config File** Toggle to *Enabled* to download config file during reboot.
- **File Name** The name of the configuration file to be downloaded.

## System Utilities

The **Utilities** menu features **Ping Test**, **Save Settings to TFTP Server**, **Save Switch History to TFTP Server**, and **Clear Address Table** commands. Additionally, this menu allows you to enable or disable Web management.

Choose **System Utilities** on the main menu to access the **Utilities** menu seen below:

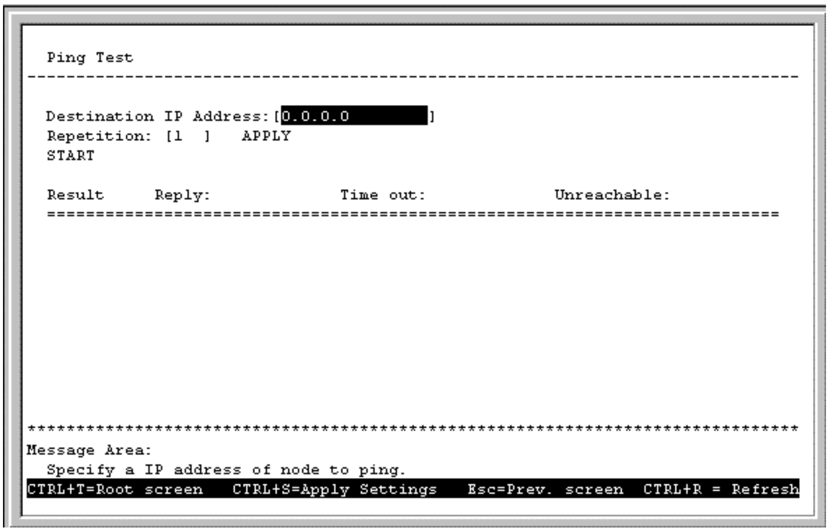


```
  Utilities
--------------------------------------------------------------------------------

  Ping Test
  Save Settings to TFTP Server
  Save Switch History to TFTP Server
  Clear Address Table

  WEB Management<Enabled >     APPLY

********************************************************************************
Message Area:
  Query a specified address.
CTRL+T=Root screen            Esc=Prev. screen                CTRL+R = Refresh
```

Figure 6-46. Utilities menu

## Ping Test

Choose **Ping Test** to access the following screen:



```
  Ping Test
--------------------------------------------------------------------------------

  Destination IP Address:[0.0.0.0         ]
  Repetition: [1  ]   APPLY
  START

  Result     Reply:             Time out:            Unreachable:
  ===========================================================================

********************************************************************************
Message Area:
  Specify a IP address of node to ping.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-47. Ping Test screen

A ping test sends out a PING (Packet INternet Groper) packet to test network connectivity between the Switch and any other network device with an IP address.

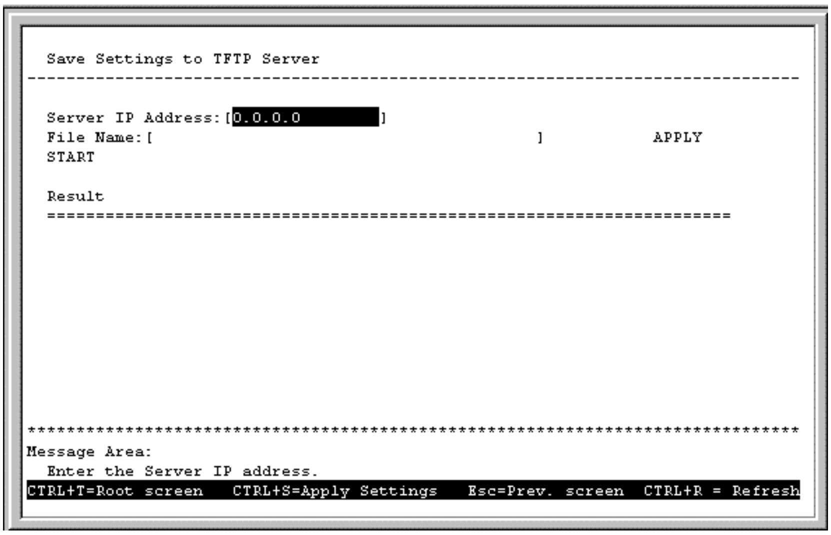
The fields you can set are:

- **Destination IP Address** The IP address to be Pinged.
- **Repetition** Amount of times the Switch should send the Ping (1-255). If zero is chosen, the Switch will continue Pinging indefinitely.

In the lower part of the **Ping Test** screen, you can view the Ping status, including Result, Reply, Time out, and Unreachable.

## Save Settings to TFTP Server

You can command the Switch to transmit a copy of its current configuration settings to any TFTP server on the network. This is done by choosing **Save Settings to TFTP Server** from the **Utilities** menu. You will first be asked if you want to save the current configuration (including any recent, possibly unsaved changes) to the Switch’s non-volatile memory; then the following screen will appear:



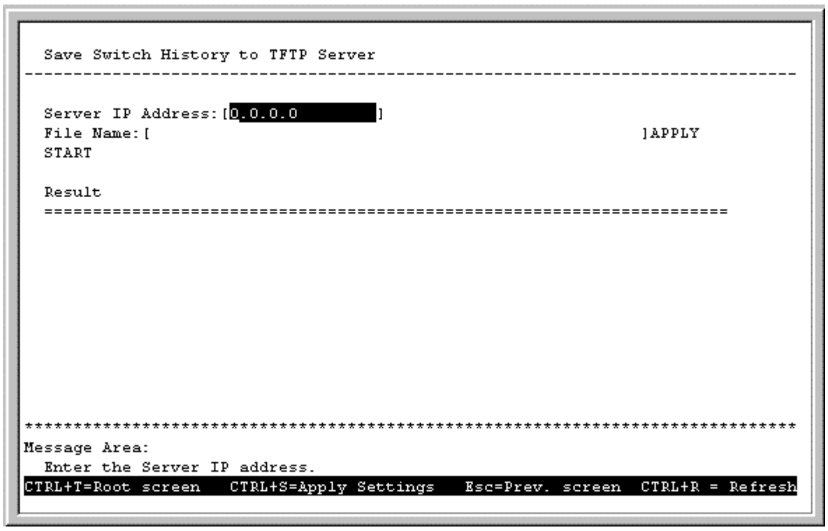
```
  Save Settings to TFTP Server
-------------------------------------------------------------------------------

  Server IP Address:[0.0.0.0          ]
  File Name:[                                      ]           APPLY
  START

  Result
  ======================================================================









*******************************************************************************
Message Area:
  Enter the Server IP address.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-48. Save Settings to TFTP Server screen

To upload the current configuration settings from the Switch to a TFTP server, enter the server’s IP address and a suitable file name, then choose START. The result will be reported in the lower part of the screen.

## Save Switch History to TFTP Server

The **Save Switch History to TFTP Server** function lets you command the Switch to send a record of operational events (see **Switch History** under **Network Monitoring**, further on in this chapter) to any TFTP server on the network. Choose this function to display the following screen:



```
  Save Switch History to TFTP Server
-------------------------------------------------------------------------------

  Server IP Address:[0.0.0.0          ]
  File Name:[                                                ]APPLY
  START

  Result
  ======================================================================









*******************************************************************************
Message Area:
  Enter the Server IP address.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

Figure 6-49. Save Switch History to TFTP Server screen

To upload Switch history to a TFTP server, enter the server’s IP address and a suitable file name, then choose START. The result will be reported in the lower part of the screen.

### Clear Address Table

Choose **Clear Address Table** from the **Utilities** menu (under **System Utilities** on the main menu) to clear the entire Address Table (also known as the Filtering and Forwarding table).

## *SNMP Manager Configuration*

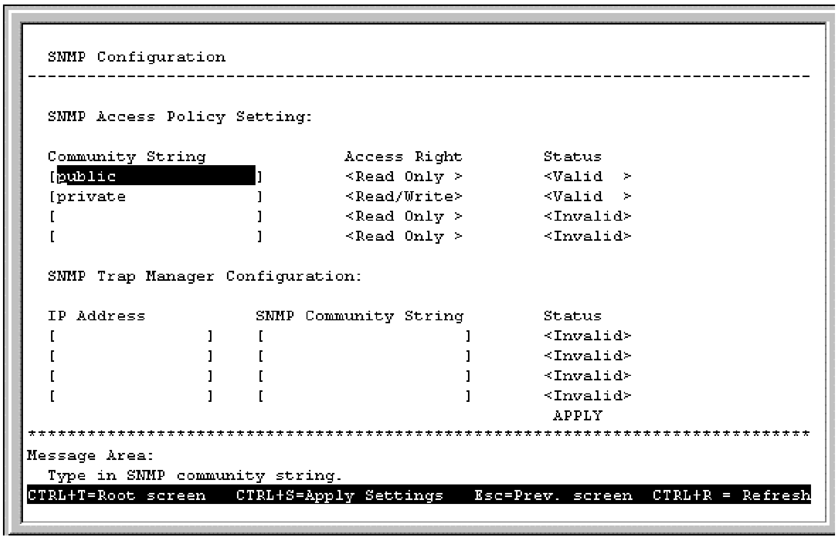
The Switch sends out SNMP *traps* to network management stations whenever certain exceptional events occur, such as when the Switch is turned on or when a system reset occurs. The Switch allows traps to be routed to up to four different network management hosts.

For a detailed list of Trap Types used for this Switch, see the *Traps* section of Chapter 5, "*Switch Management Concepts*."

SNMP (version 1) implements a rudimentary form of security by requiring that each request include a *community name*. A community name is an arbitrary string of characters used as a "password" to control access to the Switch. If the Switch receives a request with a community name it does not recognize, it will trigger an authentication trap.

The SNMP allows up to four different community names to be defined. The community name `public` is defined by default; you can change this name in addition to adding others. You will need to coordinate these names with the community name settings you use in your network management system.

Choose **SNMP Manager Configuration** from the main menu to access the following screen:



```
  SNMP Configuration
--------------------------------------------------------------------------------

  SNMP Access Policy Setting:

  Community String              Access Right        Status
  [public              ]        <Read Only >        <Valid  >
  [private             ]        <Read/Write>        <Valid  >
  [                    ]        <Read Only >        <Invalid>
  [                    ]        <Read Only >        <Invalid>

  SNMP Trap Manager Configuration:

  IP Address           SNMP Community String        Status
  [               ]    [                    ]       <Invalid>
  [               ]    [                    ]       <Invalid>
  [               ]    [                    ]       <Invalid>
  [               ]    [                    ]       <Invalid>
                                                     APPLY
********************************************************************************
Message Area:
  Type in SNMP community string.
CTRL+T=Root screen   CTRL+S=Apply Settings   Esc=Prev. screen  CTRL+R = Refresh
```

**Figure 6-50. SNMP Configuration screen**

The following parameters can be set:

- **Community String/SNMP Community String** Determines the community name to be included in the trap request.
- **Access Right** Allows each community to be separately set to either *Read Only* or *Read/Write*.
- **Status** Determines whether this community name entry is *Valid* or *Invalid*. An entry can be deleted by changing its status to *Invalid*.
- **IP Address** The IP address of the network management station to receive the trap.

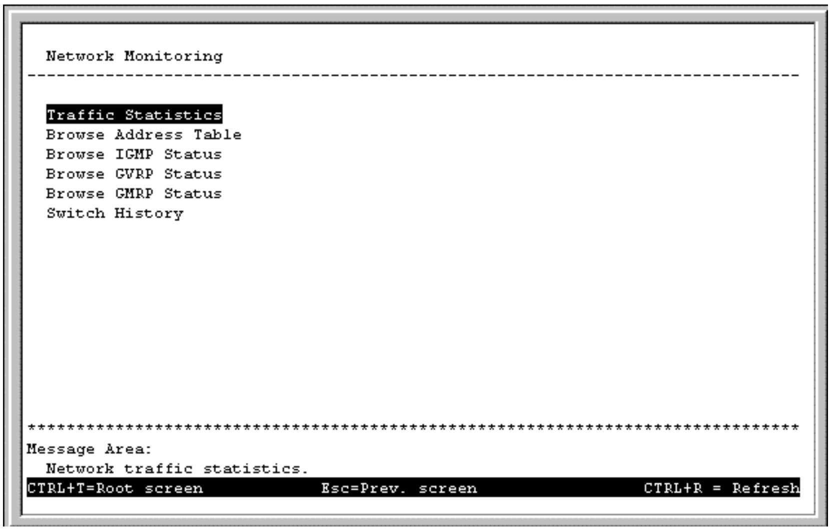
# Switch Monitoring

The Switch uses an SNMP agent which monitors different aspects of network traffic. The SNMP agent keeps counters and statistics on the operation of the Switch itself, and on each port on the Switch. The statistics obtained can be used to monitor the conditions and general efficiency of the Switch.

## *Network Monitoring*

The **Network Monitoring** menu offers six items, **Traffic Statistics**, **Browse Address Table**, **Browse IGMP Status**, **Browse GVRP Status**, **Browse GMRP Status**, and **Switch History**.

Choose **Network Monitoring** from the main menu. The following menu appears.



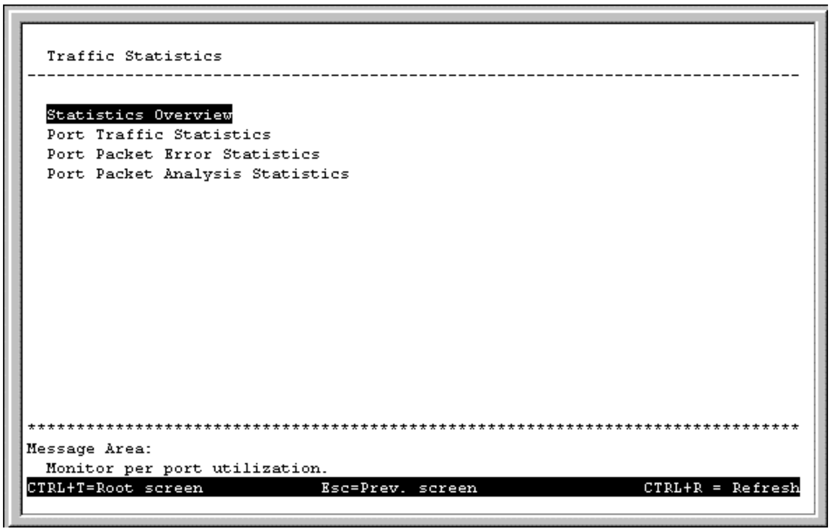
```
  Network Monitoring
-------------------------------------------------------------------------------

  Traffic Statistics
  Browse Address Table
  Browse IGMP Status
  Browse GVRP Status
  Browse GMRP Status
  Switch History









*******************************************************************************
Message Area:
  Network traffic statistics.
CTRL+T=Root screen          Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-51. Network Monitoring menu

The first item on this menu permits you to access four different tables that observe the condition of each individual port.

### Traffic Statistics

To display the **Traffic Statistics** menu, choose the first item on the **Network Monitorin**g menu. The following menu appears:

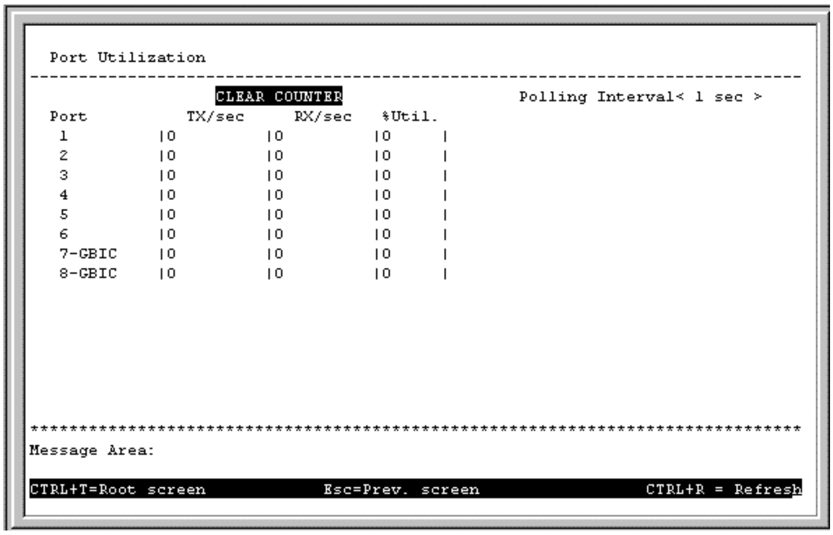


```
  Traffic Statistics
--------------------------------------------------------------------------------

  Statistics Overview
  Port Traffic Statistics
  Port Packet Error Statistics
  Port Packet Analysis Statistics











********************************************************************************
Message Area:
  Monitor per port utilization.
CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-52. Traffic Statistics menu

### Statistics Overview

To access the first item on the **Traffic Statistics** menu, choose **Statistics Overview**. The following table appears:



```
  Port Utilization
--------------------------------------------------------------------------------
                   CLEAR COUNTER                         Polling Interval< 1 sec >
  Port           TX/sec      RX/sec    %Util.
   1          |0          |0          |0     |
   2          |0          |0          |0     |
   3          |0          |0          |0     |
   4          |0          |0          |0     |
   5          |0          |0          |0     |
   6          |0          |0          |0     |
   7-GBIC     |0          |0          |0     |
   8-GBIC     |0          |0          |0     |






********************************************************************************
Message Area:

CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

Figure 6-53. Port Utilization screen

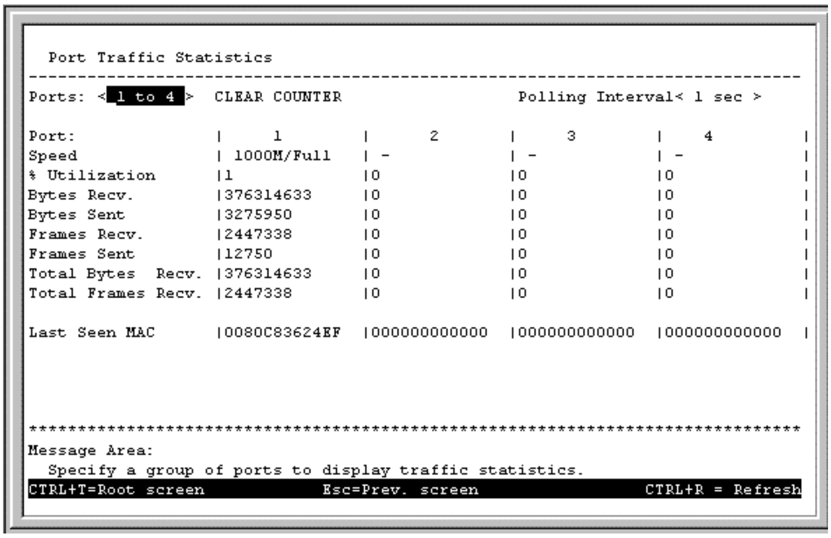
The information displayed above includes:

- **Polling Interval** Select the desired update increment setting from: *1 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.
- **TX/sec** The number of good bytes sent from the respective port per second.
- **RX/sec** The number of good bytes received per second. This also includes local and dropped packets.
- **%Util.** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval.

Press CLEAR COUNTER to reset all statistic counters on this screen.

### Port Traffic Statistics

To access the second item on the **Traffic Statistics** menu, choose **Port Traffic Statistics**. The following table appears:



```
  Port Traffic Statistics
--------------------------------------------------------------------------------
Ports: < 1 to 4 >  CLEAR COUNTER                Polling Interval< 1 sec >

Port:              |     1      |      2      |     3      |    4        |
Speed              | 1000M/Full | -           | -          | -           |
% Utilization      |1           |0            |0           |0            |
Bytes Recv.        |376314633   |0            |0           |0            |
Bytes Sent         |3275950     |0            |0           |0            |
Frames Recv.       |2447338     |0            |0           |0            |
Frames Sent        |12750       |0            |0           |0            |
Total Bytes  Recv. |376314633   |0            |0           |0            |
Total Frames Recv. |2447338     |0            |0           |0            |

Last Seen MAC      |0080C83624EF |000000000000 |000000000000 |000000000000  |




********************************************************************************
Message Area:
  Specify a group of ports to display traffic statistics.
CTRL+T=Root screen           Esc=Prev. screen                 CTRL+R = Refresh
```

**Figure 6-54. Port Traffic Statistics screen**

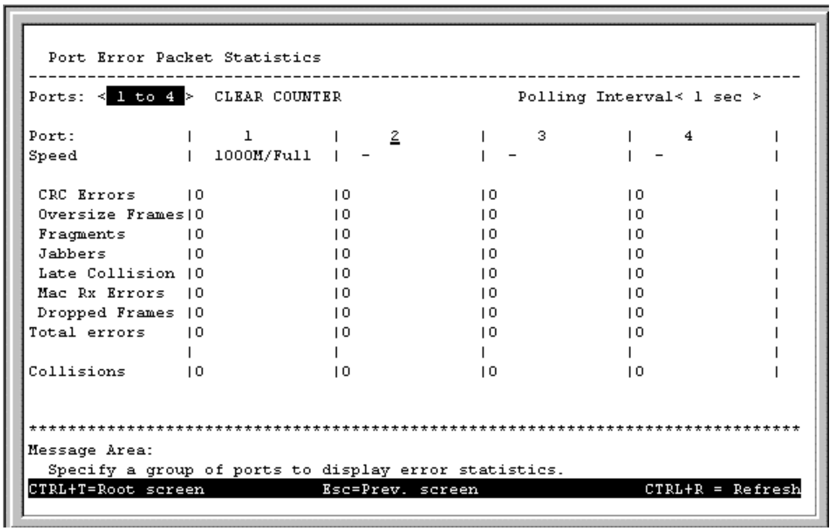
The information displayed above includes:

- **Ports** This field always displays either "*1 to 4*" or "*5 to 8*" in this 8-port switch version.
- **Polling Interval** Select the desired update increment setting from: *1 sec, 5 sec, 15 sec, 30 sec, 1 min*, or *Suspend*.
- **Speed** The speed of a specific port. When a link is down, "–" is displayed.
- **% Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval.
- **Bytes Recv.** The number of good bytes received. This also includes local and dropped packets.
- **Bytes Sent** The number of good bytes sent from the respective port.
- **Frames Recv.** The number of good frames received. This also includes local and dropped packets.
- **Frames Sent** The number of good frames sent from the respective port.
- **Total Bytes Recv.** The number of bytes received, good and bad.
- **Total Frames Recv.** The number of frames received, good and bad.
- **Last Seen MAC** The MAC address of the device where the port information was most recently accessed.

Press CLEAR COUNTER to reset all statistic counters on this screen.

### Port Packet Error Statistics

To access the third item on the **Traffic Statistics** menu, choose **Port Packet Error Statistics**. The following table appears:



```
  Port Error Packet Statistics
-------------------------------------------------------------------------------
Ports: < 1 to 4 >  CLEAR COUNTER                 Polling Interval< 1 sec >

Port:           |    1         |     2        |     3        |     4        |
Speed           |  1000M/Full  |  -           |  -           |  -           |

 CRC Errors     |0             |0             |0             |0             |
 Oversize Frames|0             |0             |0             |0             |
 Fragments      |0             |0             |0             |0             |
 Jabbers        |0             |0             |0             |0             |
 Late Collision |0             |0             |0             |0             |
 Mac Rx Errors  |0             |0             |0             |0             |
 Dropped Frames |0             |0             |0             |0             |
Total errors    |0             |0             |0             |0             |
                |              |              |              |              |
Collisions      |0             |0             |0             |0             |


*******************************************************************************
Message Area:
  Specify a group of ports to display error statistics.
CTRL+T=Root screen          Esc=Prev. screen                    CTRL+R = Refresh
```

**Figure 6-55. Port Error Packet Statistics screen**

The information displayed above includes:

- **Ports** This field always displays either "*1 to 4*" or "*5 to 8*" in this 8-port switch version.

- **Polling Interval** Select the desired update increment setting from: *1 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.

- **CRC Errors** The number of frames that fail the CRC integrity check.

- **Oversize Frames** The number of good frames with length greater than 1518 bytes and therefore are greater than the maximum legal length.

- **Fragments** The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

- **Jabbers** The number of frames with length more than 1518 bytes and with CRC error or misalignment (bad framing).

- **Late Collision** The number of collisions that occur at or after the 64th byte (octet) in the frame.

- **Mac Rx Errors** The number of frames with received MAC Errors.

- **Dropped Frames** Counts received packets which are dropped due to any of the following reasons: lack of available receive buffers, port-disable, link-test-fail, spanning tree, or empty distribution list.

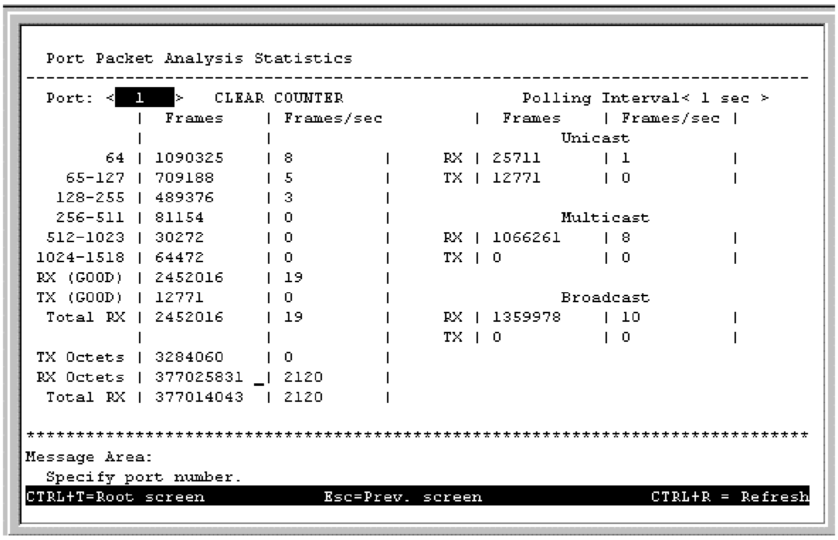
- **Total errors** The sum of the CRC Errors, Oversize Frames, Fragments, Jabbers, Late Collision, Mac Rx Errors, and Dropped Frames counters.

- **Collisions** The number of collision errors.

Press CLEAR COUNTER to reset all statistic counters on this screen.

### *Port Packet Analysis Statistics*

To access the fourth item on the **Traffic Statistics** menu, choose **Port Packet Analysis Statistics**. The following table appears:



```
  Port Packet Analysis Statistics
-------------------------------------------------------------------------------
  Port: <  1   >   CLEAR COUNTER                 Polling Interval< 1 sec >
           |  Frames     | Frames/sec          |  Frames     | Frames/sec |
           |             |                           Unicast
        64 | 1090325     | 8           |     RX | 25711       | 1           |
    65-127 | 709188      | 5           |     TX | 12771       | 0           |
   128-255 | 489376      | 3           |
   256-511 | 81154       | 0           |               Multicast
  512-1023 | 30272       | 0           |     RX | 1066261     | 8           |
 1024-1518 | 64472       | 0           |     TX | 0           | 0           |
 RX (GOOD) | 2452016     | 19          |
 TX (GOOD) | 12771       | 0           |               Broadcast
  Total RX | 2452016     | 19          |     RX | 1359978     | 10          |
           |             |             |     TX | 0           | 0           |
 TX Octets | 3284060     | 0           |
 RX Octets | 377025831  _| 2120        |
  Total RX | 377014043   | 2120        |

*******************************************************************************
Message Area:
  Specify port number.
CTRL+T=Root screen           Esc=Prev. screen                 CTRL+R = Refresh
```

**Figure 6-56. Port Packet Analysis Statistics screen**

The information displayed above includes:

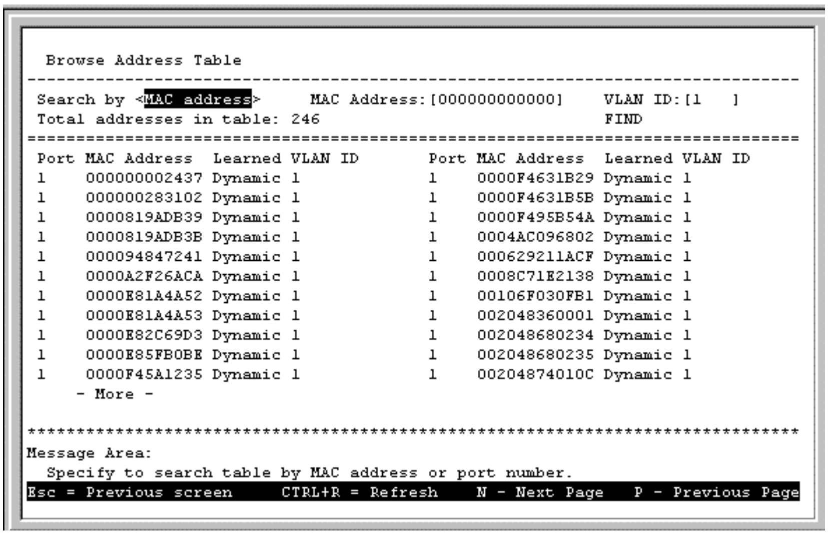
- **Port** Enter the desired port in this field.
- **Polling Interval** Select the desired update increment setting from: *1 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.
- **64**, **65-127**, **128-255**, **256-511**, **512-1023**, **1024-1518** The number of good frames of various length ranges, both valid and invalid.
- **RX (GOOD)** The number of good frames received. This also includes local and dropped packets.
- **TX (GOOD)** The number of good frames sent from the respective port.
- **Total RX** The number of frames received, good and bad.
- **TX Octets** The number of good bytes sent from the respective port.
- **RX Octets** The number of good bytes received. This also includes local and dropped packets.
- **Total RX** The number of bytes received, good and bad.
- **Unicast RX/Unicast TX** The number of good unicast frames received and sent. This includes dropped unicast packets.
- **Multicast RX/Multicast TX** The number of good multicast frames received and sent. This includes local and dropped multicast packets.
- **Broadcast RX/Broadcast TX** The number of good broadcast frames received and sent. This includes dropped broadcast packets.

Press CLEAR COUNTER to reset all statistic counters on this screen.

## Browse Address Table

The **Browse Address Table** screen allows the user to view which Switch port(s) a specific network device uses to communicate on the network. You can sort this table by MAC address, port, VLAN ID, and sequence. This is useful for viewing which ports one device is using, or which devices are using one port.

To display the **Browse Address Table** screen, choose **Network Monitoring** from the main menu and then choose **Browse Address Table**. The following screen appears:



```
 Browse Address Table
--------------------------------------------------------------------------------
 Search by <MAC address>     MAC Address:[000000000000]     VLAN ID:[1    ]
 Total addresses in table: 246                              FIND
================================================================================
 Port MAC Address  Learned VLAN ID       Port MAC Address  Learned VLAN ID
 1    000000002437 Dynamic 1             1    0000F4631B29 Dynamic 1
 1    000000283102 Dynamic 1             1    0000F4631B5B Dynamic 1
 1    0000819ADB39 Dynamic 1             1    0000F495B54A Dynamic 1
 1    0000819ADB3B Dynamic 1             1    0004AC096802 Dynamic 1
 1    000094847241 Dynamic 1             1    000629211ACF Dynamic 1
 1    0000A2F26ACA Dynamic 1             1    0008C71E2138 Dynamic 1
 1    0000E81A4A52 Dynamic 1             1    00106F030FB1 Dynamic 1
 1    0000E81A4A53 Dynamic 1             1    002048360001 Dynamic 1
 1    0000E82C69D3 Dynamic 1             1    002048680234 Dynamic 1
 1    0000E85FB0BE Dynamic 1             1    002048680235 Dynamic 1
 1    0000F45A1235 Dynamic 1             1    00204874010C Dynamic 1
     - More -

********************************************************************************
Message Area:
  Specify to search table by MAC address or port number.
Esc = Previous screen     CTRL+R = Refresh    N - Next Page   P - Previous Page
```

**Figure 6-57.  Browse Address Table**

To browse by MAC address, select *MAC address* in the Search by field, enter the desired MAC address in the next field, enter a VLAN ID in the following field, and then press FIND.

To browse by port number, select *Port* in the Search by field, enter the desired port in the next field, enter a VVLAN ID in the following field, and then press FIND.

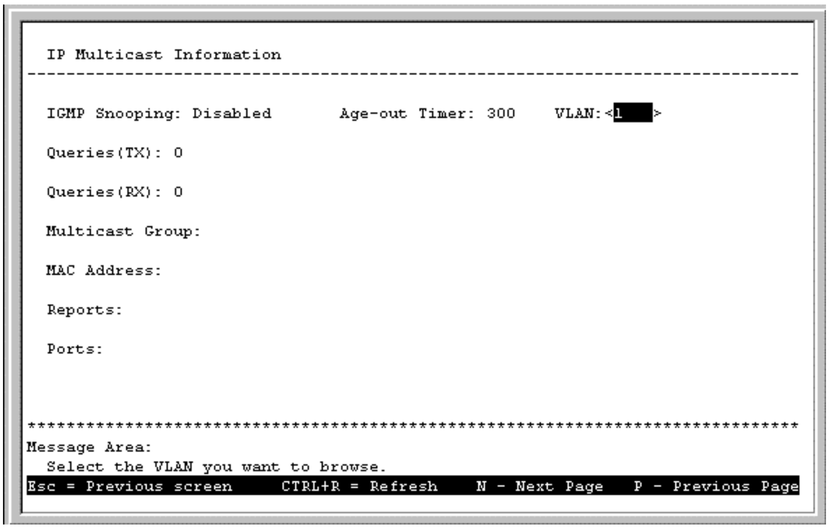
To browse by VLAN ID, select *VLAN* in the Search By field, enter the desired VLAN ID in the field offered, and then press FIND.

A forwarding table containing Port, MAC Address, Learned status, and VLAN ID is located on the lower part of the screen.

## Browse IGMP Status

The Browse IGMP Status function allows you to browse Internet Group Management Protocol (IGMP). The Switch is able to recognize IGMP queries and reports sent between stations and an IGMP router. When enabled for IGMP snooping, the Switch can open or close a port to specific devices based on the IGMP messages sent from the device to the router or vice versa.

To display the **IP Multicast Information** screen, choose **Network Monitoring** from the main menu and then choose **Browse IGMP Status**. The following screen appears:



```
 IP Multicast Information
-------------------------------------------------------------------------------

 IGMP Snooping: Disabled       Age-out Timer: 300    VLAN:<1   >

 Queries(TX): 0

 Queries(RX): 0

 Multicast Group:

 MAC Address:

 Reports:

 Ports:


*******************************************************************************
Message Area:
 Select the VLAN you want to browse.
Esc = Previous screen     CTRL+R = Refresh    N - Next Page   P - Previous Page
```

**Figure 6-58. IP Multicast Information screen**

This screen displays the number of IGMP queries and reports for each active IP multicast group detected by the Switch. You can also view which Switch ports support each multicast group.

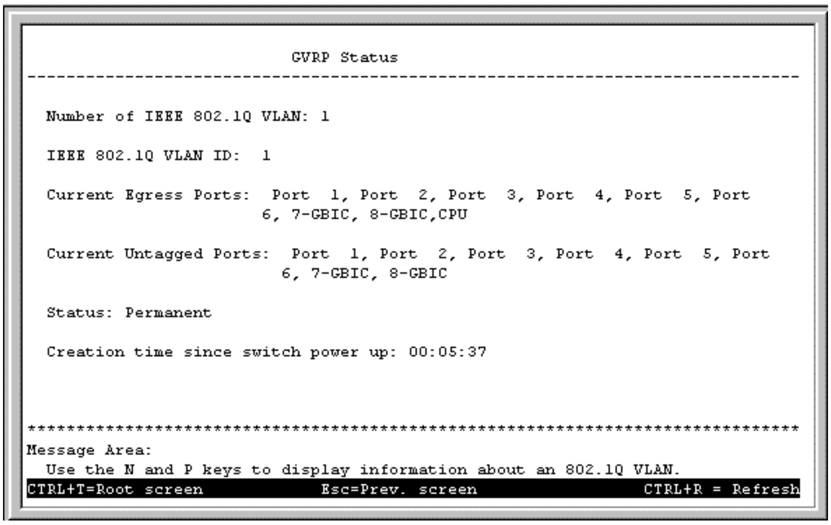
The fields displayed are defined as follows:

- **IGMP Snooping** Indicates whether IGMP snooping is *Enabled* or *Disabled*.
- **Age-out Timer** Displays the time the Switch waits between IGMP queries.
- **VLAN** Enter the desired VLAN ID number in this field.
- **Queries(TX)** The number of IGMP requests sent by the switch.
- **Queries(RX)** The number of IGMP requests that have arrived at a switch port.
- **Multicast Group** The Multicast IP address of the Multicast group being displayed.
- **MAC Address** The Multicast MAC address of the multicast group being displayed.
- **Reports** The number of notifications sent from each station to the IGMP host, signifying that the station is still (or wants to be) part of a multicast group.
- **Ports** The Switch ports supporting the selected multicast group.

## Browse GVRP Status

The **GVRP Status** screen allows you to browse GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP).

To display the **GVRP Status** screen, choose **Network Monitoring** from the main menu and then choose **Browse GVRP Status**. The following screen appears:



```
                          GVRP Status
-------------------------------------------------------------------------------

  Number of IEEE 802.1Q VLAN: 1

  IEEE 802.1Q VLAN ID:  1

  Current Egress Ports:  Port  1, Port  2, Port  3, Port  4, Port  5, Port
                       6, 7-GBIC, 8-GBIC,CPU

  Current Untagged Ports:  Port  1, Port  2, Port  3, Port  4, Port  5, Port
                         6, 7-GBIC, 8-GBIC

  Status: Permanent

  Creation time since switch power up: 00:05:37



*******************************************************************************
Message Area:
  Use the N and P keys to display information about an 802.1Q VLAN.
CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

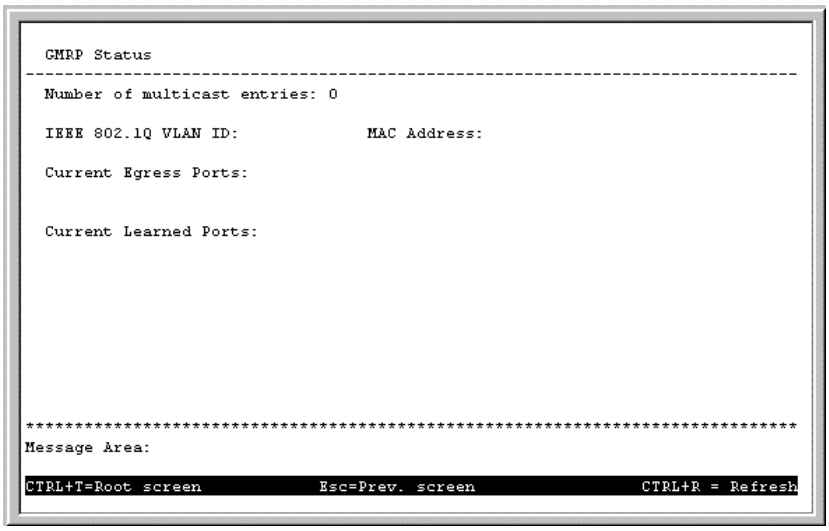
Figure 6-59.  GVRP Status screen

This screen contains information pertaining to GVRP. Press N to view the status of additional IEEE 802.1Q VLANs.

## Browse GMRP Status

The **GMRP Status** screen allows you to browse Group Multicast Registration Protocol (GMRP).

To display the **GMRP Status** screen, choose **Network Monitoring** from the main menu and then choose **Browse GMRP Status**. The following screen appears:



```
  GMRP Status
-------------------------------------------------------------------------------
  Number of multicast entries: 0

  IEEE 802.1Q VLAN ID:             MAC Address:

  Current Egress Ports:


  Current Learned Ports:










*******************************************************************************
Message Area:

CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

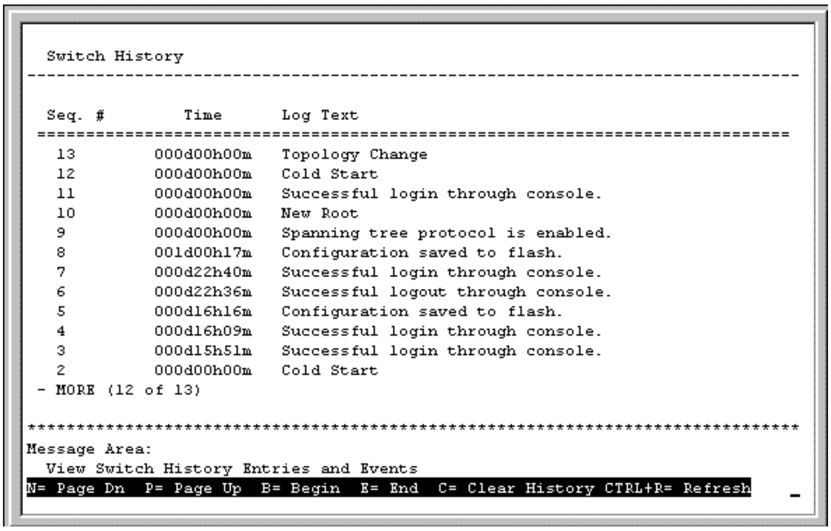
Figure 6-60.  GMRP Status screen

This screen contains information pertaining to the GMRP status of IEEE 802.1Q VLANs.

## Switch History

The Switch keeps a record of events that may be of interest to a network administrator: startups, reconfigurations, link activations and deactivations, firmware upgrades, and others.

To view this record, choose **Network Monitoring** from the main menu, and then choose **Switch History** from the **Network Monitoring** menu. A screen similar to that shown below will appear:



```
  Switch History
------------------------------------------------------------------------------

  Seq. #        Time      Log Text
 ============================================================================
   13        000d00h00m   Topology Change
   12        000d00h00m   Cold Start
   11        000d00h00m   Successful login through console.
   10        000d00h00m   New Root
    9        000d00h00m   Spanning tree protocol is enabled.
    8        001d00h17m   Configuration saved to flash.
    7        000d22h40m   Successful login through console.
    6        000d22h36m   Successful logout through console.
    5        000d16h16m   Configuration saved to flash.
    4        000d16h09m   Successful login through console.
    3        000d15h51m   Successful login through console.
    2        000d00h00m   Cold Start
 - MORE (12 of 13)

******************************************************************************
Message Area:
  View Switch History Entries and Events
N= Page Dn  P= Page Up  B= Begin  E= End  C= Clear History CTRL+R= Refresh
```

**Figure 6-61. Switch History screen**

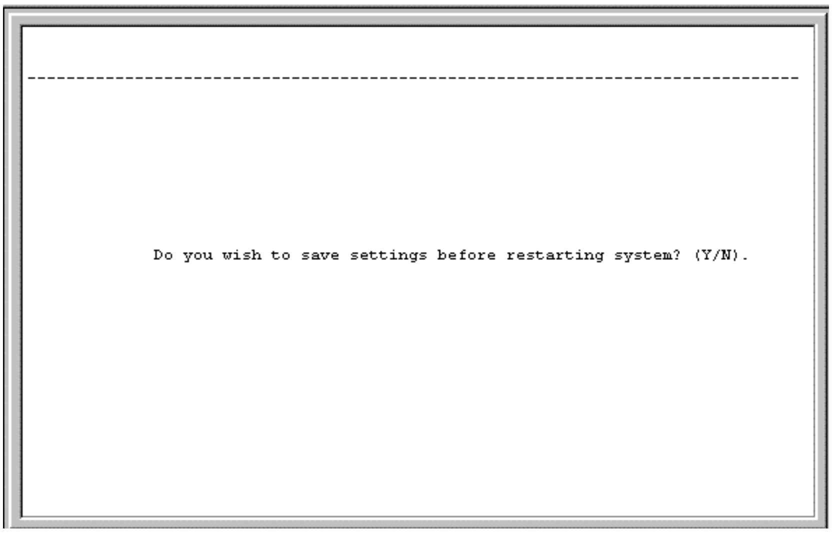
The Switch can be commanded to upload its history via TFTP to a machine you specify. See *System Utilities* earlier in this chapter.

# Resetting the Switch

You can use the console interface to reset the Switch, either doing a Restart System (which restarts the Switch and is identical to powering the Switch off and back on again) or a Factory Reset to Default Value (which sets all of the Switch’s parameters to what they were when the Switch was delivered from the factory).

## *Restart System*

To perform a system reset, choose **Restart System** from the main menu. The following screen will appear:



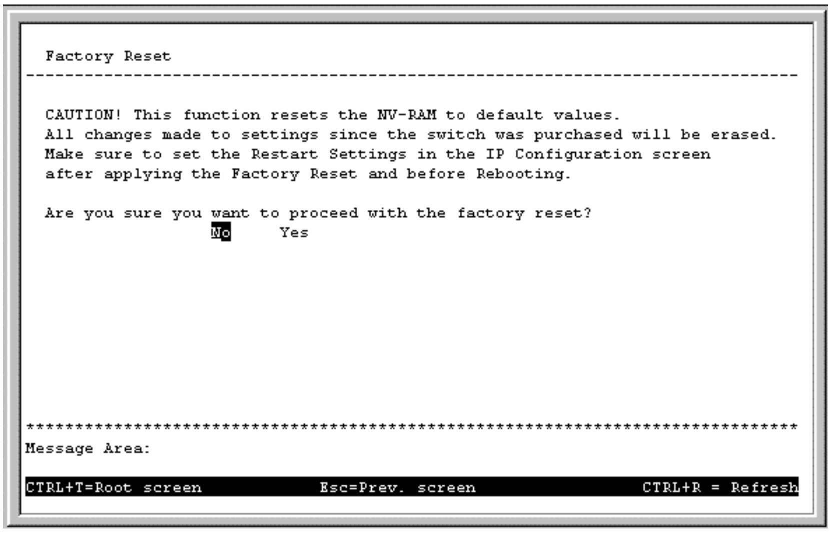
```
------------------------------------------------------------------------------



             Do you wish to save settings before restarting system? (Y/N).
```

**Figure 6-62. Restart System screen**

## Factory Reset

Before performing a factory reset, be absolutely certain that this is what you want to do. Once the reset is done, all of the Switch's settings stored in NV-RAM (including TCP/IP parameters, SNMP parameters, the enabled/disabled settings of ports, security settings, etc.) will be erased and restored to their factory default settings.

**1.** Choose **Factory Reset** from the main menu. The following screen appears:



```
  Factory Reset
-------------------------------------------------------------------------------

  CAUTION! This function resets the NV-RAM to default values.
  All changes made to settings since the switch was purchased will be erased.
  Make sure to set the Restart Settings in the IP Configuration screen
  after applying the Factory Reset and before Rebooting.

  Are you sure you want to proceed with the factory reset?
                   No      Yes









*******************************************************************************
Message Area:

CTRL+T=Root screen            Esc=Prev. screen                 CTRL+R = Refresh
```

**Figure 6-63. Factory Reset screen**

**2.** Move the cursor to Yes to confirm the reset and press <Enter>. The main menu screen should appear.

## Logout

To exit the Switch, choose **Logout** from the main menu. You will be returned to the opening login screen.

# 7

# WEB-BASED NETWORK MANAGEMENT

## Introduction

The DGS-3208TG offers an embedded Web-based (hypertext) interface allowing users to manage the Switch from anywhere on the network through a standard browser such as Netscape Navigator/Communicator or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the Switch using HTTP protocol. Your browser screen may differ from the screen shots (pictures) in this guide.

***Note:*** This Web-based network management module does not accept Chinese language input (or other languages requiring 2 bytes per character).

## Getting Started

The first step in getting started in using Web-based management for your Switch is to secure a browser. A Web browser is a program which allows a person to read hypertext, for example, Netscape Navigator or Microsoft Internet Explorer. Follow the installation instructions for the browser.

The second and last step is to configure the IP interface of the Switch. This can be done manually through a console (see the *Configure IP Address* section in the "*Using The Console Interface*" chapter).

## Management

To begin managing your Switch simply run the browser you have installed on your computer and open the IP address you have defined for the device.

In the page that opens, click on the *Login to DGS-3200 Manager* hyperlink:

This opens the main page in the management module, shown below in the section entitled *Basic Setup*.

The top portion of the window contains an interactive view of the Switch's front panel. Clicking on one of the eight ports opens a configuration window for that particular port.

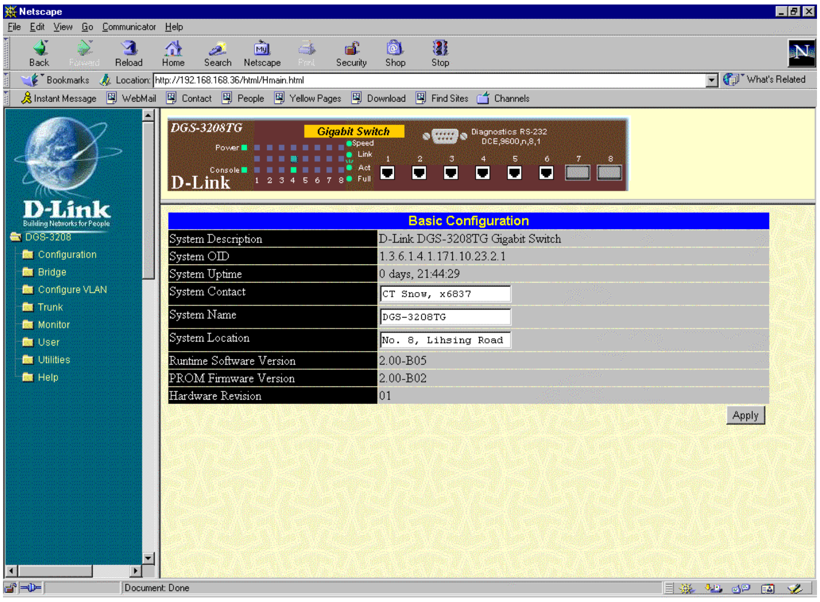
The main page contains a window along the left side with a column of folder icons labeled **Configuration**, **Bridge**, **Configure VLAN**, **Trunk**, **Monitor**, **User**, **Utilities**, and **Help**. These are the major categories for Switch management. Clicking on the icon on the far left side of each category (except **Help**, which directly connects you to a help program) causes a list of options to appear underneath the major category.

All categories and options are explained below.

# Configuration

This is the first category and is opened by default when you login to the Web-based management program. The **Configuration** options include **Basic Setup**, **TCP/IP Setup**, **Advanced**, **Ports Setup**, **Port Mirror**, **Trap Manager**, **SNMP Manager**, **Download**, **Console**, **Save**, and **Reset**. See below for explanations of each one.

## Basic Setup



Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.168.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
Power
Console
Speed
Link
Act
Full
Apply
Document: Done

| Basic Configuration | |
|---|---|
| System Description | D-Link DGS-3208TG Gigabit Switch |
| System OID | 1.3.6.1.4.1.171.10.23.2.1 |
| System Uptime | 0 days, 21:44:29 |
| System Contact | CT Snow, x6837 |
| System Name | DGS-3208TG |
| System Location | No. 8, Lihsing Road |
| Runtime Software Version | 2.00-B05 |
| PROM Firmware Version | 2.00-B02 |
| Hardware Revision | 01 |

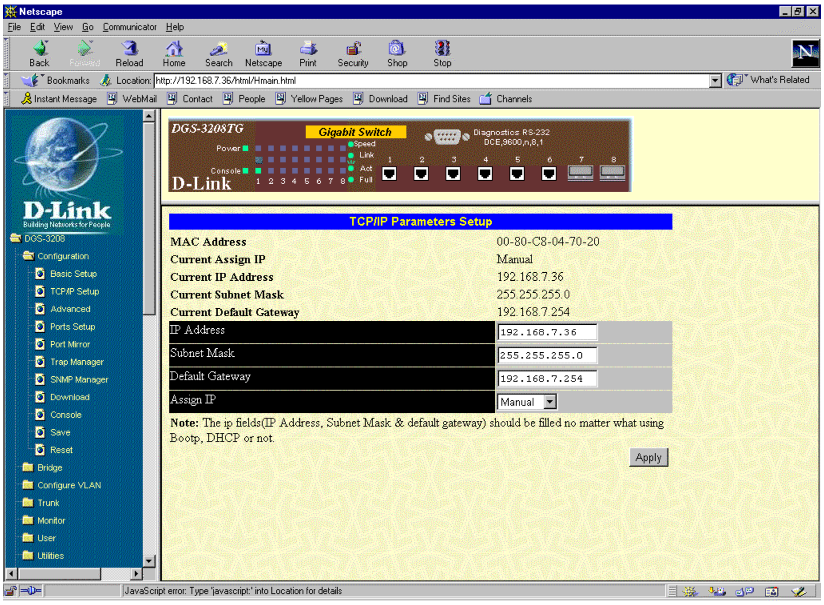
**Figure 7-1. Basic Configuration window**

To set basic Switch settings, enter the name of the person to contact should there be any problems or questions with the system in the System Contact field, a name for the system in the System Name field, and the physical location of the Switch in the System Location field. Then click **Apply**.

The remaining information in the screen includes:

- **System Description** Description of the Switch model.
- **System OID** SNMP Object Identifier for the Switch model.
- **System Uptime** Amount of time the Switch has been powered on.
- **Runtime Software Version** This version number of the software.
- **PROM Firmware Version** Version number of the firmware stored in the Flash memory of the Switch.
- **Hardware Revision** Version number of the Switch's hardware.

## TCP/IP Setup


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Basic Setup
TCP/IP Setup
Advanced
Ports Setup
Port Mirror
Trap Manager
SNMP Manager
Download
Console
Save
Reset
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
Power
Console
Speed
Link
Act
Full
1 2 3 4 5 6 7 8
D-Link
JavaScript error: Type 'javascript:' into Location for details

**TCP/IP Parameters Setup**

| | |
|---|---|
| **MAC Address** | 00-80-C8-04-70-20 |
| **Current Assign IP** | Manual |
| **Current IP Address** | 192.168.7.36 |
| **Current Subnet Mask** | 255.255.255.0 |
| **Current Default Gateway** | 192.168.7.254 |
| IP Address | 192.168.7.36 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.7.254 |
| Assign IP | Manual |

**Note:** The ip fields(IP Address, Subnet Mask & default gateway) should be filled no matter what using Bootp, DHCP or not.

Apply

**Figure 7-2. TCP/IP Parameters Setup window**

You can change the IP Address, Subnet Mask, and Default Gateway on the Switch. If you are not using BOOTP, enter the IP Address, Subnet Mask, and Default Gateway of the Switch. If you enable BOOTP, you do not need to configure any IP parameters because a BOOTP server automatically assigns IP configuration parameters to the Switch. Click **Apply** to activate the new settings.

The information is described as follows:

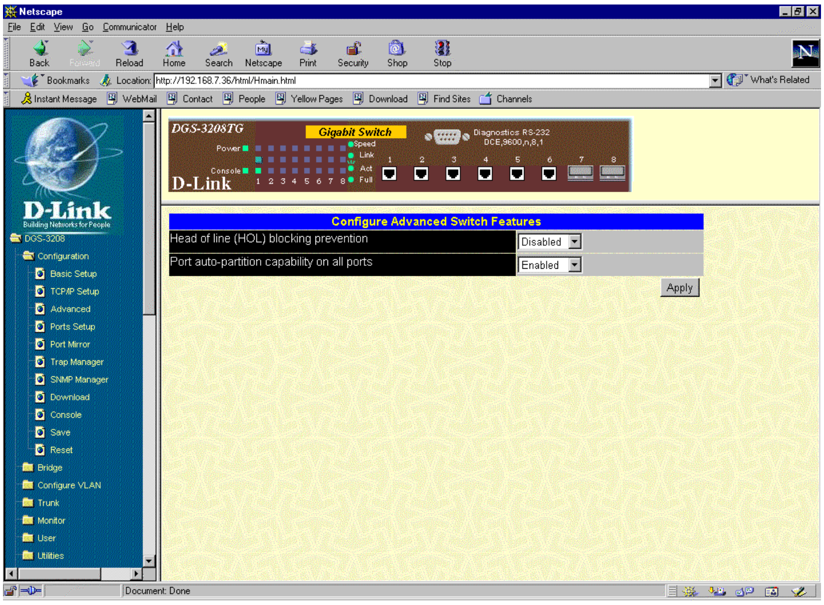
- **IP Address** The Internet address for the device.

- **Subnet Mask** The subnet mask determines the level of the subnet that the Switch is on.

- **Default Gateway** The default router for the device.

- **Assign IP** Determines whether the Switch should get its IP Address settings from the user (*Manual*), a *BOOTP* server, or a *DHCP* server. If *Manual* is chosen, the Switch will use the IP Address, Subnet Mask and Default Gateway settings defined in this screen upon being rebooted. If *BOOTP* is chosen, 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 supplied settings. If *DHCP* is chosen, a Dynamic Host Configuration Protocol request will be sent when the Switch is powered up.

## Advanced



Configure Advanced Switch Features

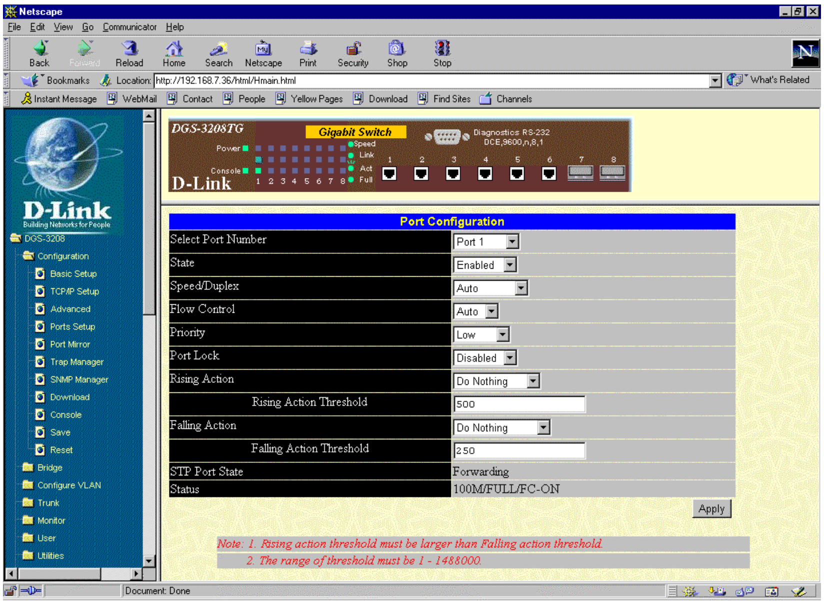
|  |  |
|---|---|
| Head of line (HOL) blocking prevention | Disabled |
| Port auto-partition capability on all ports | Enabled |

Apply

Figure 7-3. Configure Advanced Switch Features window

The Switch features head of line (HOL) blocking prevention, a function designed to prevent forwarding of a packet to a "blocking" port, that is, a port where an excess of packets are queued up. Note that when a multicast packet or a packet with an unknown destination address needs to be forwarded to several ports, and if some of them are "blocking," the packet will not be discarded, rather it will be forwarded only to the ports that are not "blocking." Toggle between *Disabled* and *Enabled* before clicking **Apply** to let your change take effect. You can also enable or disable jumbo frame support on this window.

## Ports Setup



Port Configuration

|  |  |
|---|---|
| Select Port Number | Port 1 |
| State | Enabled |
| Speed/Duplex | Auto |
| Flow Control | Auto |
| Priority | Low |
| Port Lock | Disabled |
| Rising Action | Do Nothing |
| Rising Action Threshold | 500 |
| Falling Action | Do Nothing |
| Falling Action Threshold | 250 |
| STP Port State | Forwarding |
| Status | 100M/FULL/FC-ON |

Apply

*Note: 1. Rising action threshold must be larger than Falling action threshold.*
*2. The range of threshold must be 1 - 1488000.*

Figure 7-4. Port Configuration window

Select the port you want to configure by clicking on the port in the Switch front panel display at the top of the window or by using the display above. Follow these steps:

1. Enable or disable the port. If you choose *Disabled*, devices connected to that port cannot use the Switch, and the Switch purges their addresses from its address table after the MAC address aging time elapses. The Switch won't purge addresses if you define them as permanent entries in the Forwarding Table.

2. Configure the Speed/Duplex setting for the port. The option *1000M/Full* means operation at 1000 Mbps in full duplex mode.

3. Configure the Flow Control setting for the port. Select *On* for the switch to automatically negotiate the correct flow control setting for this port. Select *Off* for no flow control.

4. Configure the Priority setting for packets passing through this port, using IEEE 802.1 tagging. Select *Normal*, *High* or *Low*. If the network is congested, the switch handles packets with a higher priority before those with lower priority.

5. Enable or disable Port Lock. Enabling Port Lock stops automatic learning for all stations connected to the port. Entries in the Forwarding Table for all devices connected to the port will age out. The only traffic this port will allow is traffic from machines whose MAC addresses are manually entered in the Static Forwarding Table.

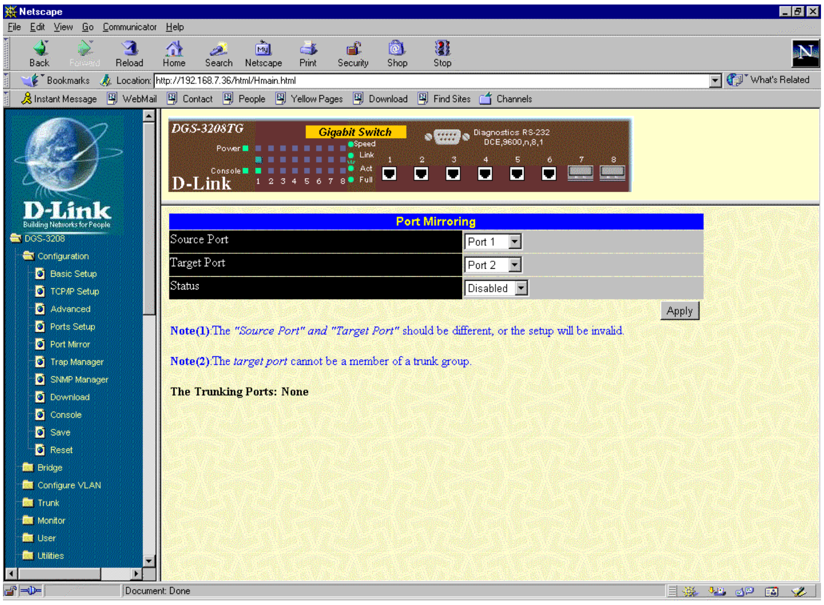
6. Specify settings for the broadcast storm controls.

   The Rising Action and Rising Action Threshold controls specify what action (if any) the Switch should take when broadcast traffic received on the port increases to or exceeds the equivalent of a specified number of broadcast packets per second. The threshold can be set to 1 to 1,488,000 packets per second (the default is 500); the rising action can be set to *Do Nothing* (this is the default), *Blocking* (that is, discard all broadcast packets received on the port), or *Blocking Trap* (discard all broadcast packets received on the port and send a trap to the trap manager[s]).

   The Falling Action and Falling Action Threshold controls specify what action (if any) the Switch should take when broadcast traffic received on the port, after reaching or exceeding the "rising action" threshold, decreases to or falls below the equivalent of a specified number of broadcast packets per second. The threshold can be set to 1 to 1,488,000 packets per second (the default is 250); the falling action can be set to *Do Nothing* (this is the default), *Forwarding* (that is, discontinue blocking of broadcast packets received on the port), or *Forwarding Trap* (discontinue blocking of broadcast packets received on the port and send a trap to the trap manager[s]).

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

## Port Mirror



Port Mirroring

| | |
|---|---|
| Source Port | Port 1 |
| Target Port | Port 2 |
| Status | Disabled |

Apply

Note(1):The *"Source Port" and "Target Port"* should be different, or the setup will be invalid.

Note(2):The *target port* cannot be a member of a trunk group.

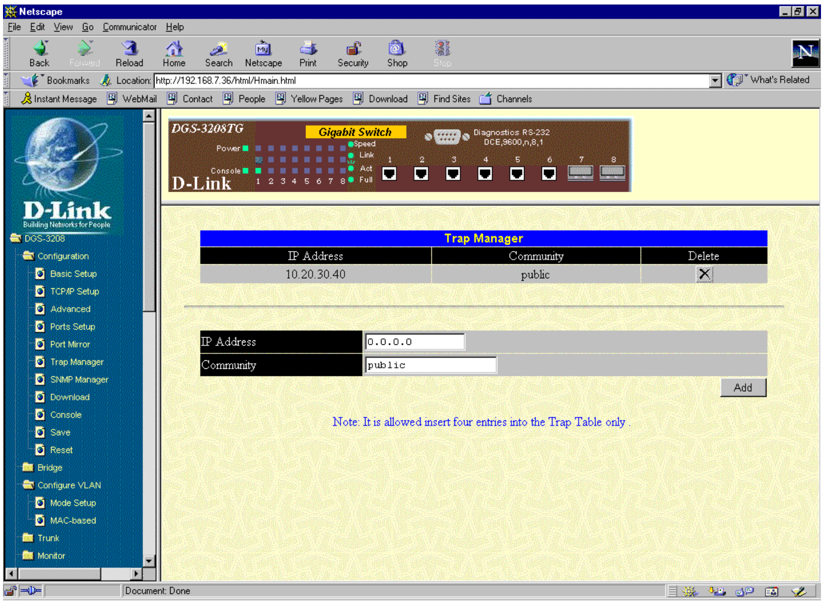
**The Trunking Ports: None**

Figure 7-5. Port Mirroring window

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

To configure a mirror port, select *Enabled* from the Status pull-down list. In the first field, select the source port from where you want to copy frames. In the second field, select the port which receives the copies from the source port. This is the port where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe.

## Trap Manager



Trap Manager

| IP Address | Community | Delete |
|---|---|---|
| 10.20.30.40 | public | ☒ |

| | |
|---|---|
| IP Address | 0.0.0.0 |
| Community | public |

Add

Note: It is allowed insert four entries into the Trap Table only .

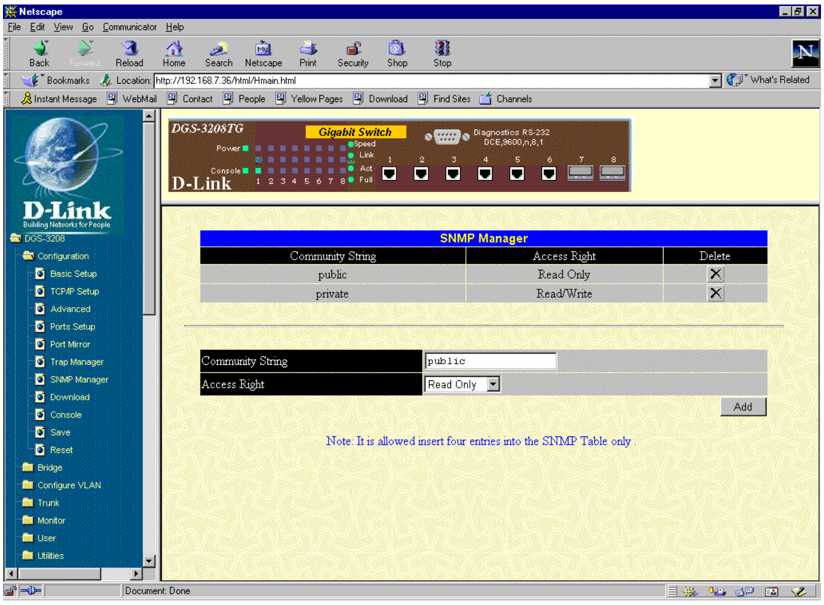
Figure 7-6. Trap Manager window

To use the trap manager function featured on this Switch, enter the desired community string and IP address of the trap receiving station (up to four are allowed). A trap receiving station is a device that constantly runs a network management application to receive and store traps. Click **Apply** to put the settings into effect

The information is described as follows:

- **IP Address** The IP address of the trap receiving station.
- **Community** A user-defined community name.

## SNMP Manager



| SNMP Manager | | |
|---|---|---|
| Community String | Access Right | Delete |
| public | Read Only | ☒ |
| private | Read/Write | ☒ |

| | |
|---|---|
| Community String | public |
| Access Right | Read Only |

Add

Note: It is allowed insert four entries into the SNMP Table only .

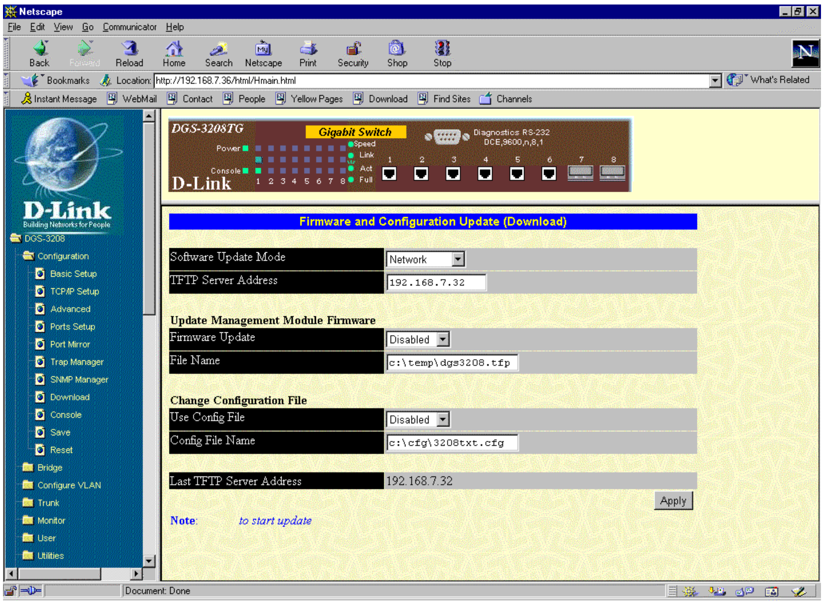
**Figure 7-7. SNMP Manager window**

To use the functions on this window, enter the desired community string for SNMP management on the Switch in the Community String field and the desired Access Right setting in the next field. You may enter up to four IP addresses of trap receiving stations in the **Trap Manager** window of the *Configuration* section. Then click **Apply** to put the settings into effect.

The information is described as follows:

- **Community String** A user-defined SNMP community name.
- **Access Right** The permitted access of *Read Only* or *Read/Write* using the SNMP community name.

## Download



Firmware and Configuration Update (Download)

| | |
|---|---|
| Software Update Mode | Network |
| TFTP Server Address | 192.168.7.32 |

Update Management Module Firmware

| | |
|---|---|
| Firmware Update | Disabled |
| File Name | c:\temp\dgs3208.tfp |

Change Configuration File

| | |
|---|---|
| Use Config File | Disabled |
| Config File Name | c:\cfg\3208txt.cfg |

| | |
|---|---|
| Last TFTP Server Address | 192.168.7.32 |

Apply

**Note:** *to start update*

**Figure 7-8. Firmware and Configuration Update (Download) window**

Firmware and configuration updating can be done from the window above. Please note that you must reboot your PC to start the update.

The information is described as follows:

♦ **Software Update Mode** Set to either *Network* or *Out of Band*. Determines whether the new firmware code should be obtained through the Ethernet network or through the console port.

♦ **TFTP Server Address** The IP address of the TFTP server where the new firmware code is.

♦ **Firmware Update** Determines whether or not the Switch should download its new firmware code the next time it is booted.

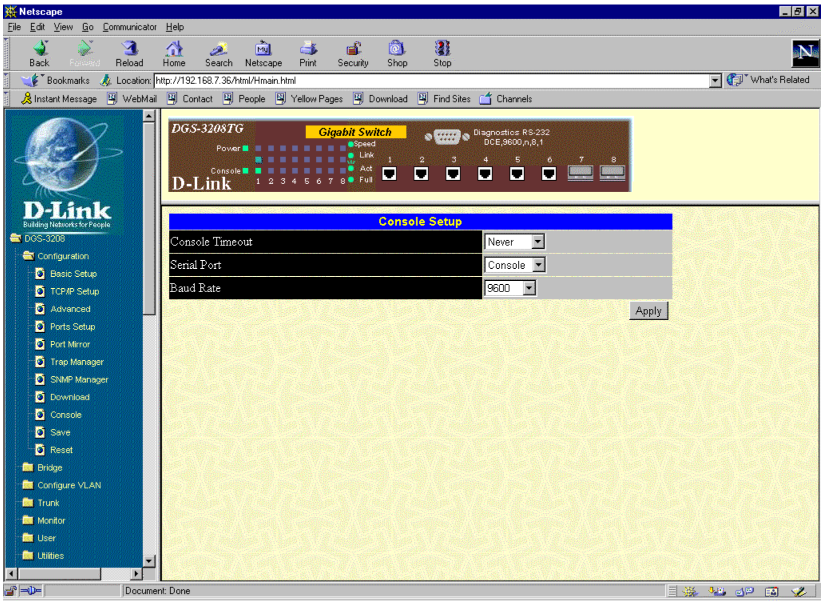
♦ **File Name** The path and the name of the file which holds the new firmware code on the TFTP server.

♦ **Use Config File** Determines whether or not the Switch should download its configuration file the next time it is booted.

♦ **Config File Name** The path and configuration name on the TFTP server.

♦ **Last TFTP Server Address** The IP address of the TFTP server where the configuration file was located in the last configuration change.

## Console



| Console Setup | |
|---|---|
| Console Timeout | Never |
| Serial Port | Console |
| Baud Rate | 9600 |

Apply

### Figure 7-9. Console Setup window

This window allows you to select the protocol for communicating through the console port, *Console* or *Slip*, in the Serial Port field. Use SLIP for out-of-band management. You can also specify the refresh rate in the Console Timeout field and the desired setting in the Baud Rate field. Click **Apply** and then reboot the Switch for console port settings to take effect.

The default serial port settings are:

Baud Rate=9600

Data Bits=8

Flow Control=XON/XOFF

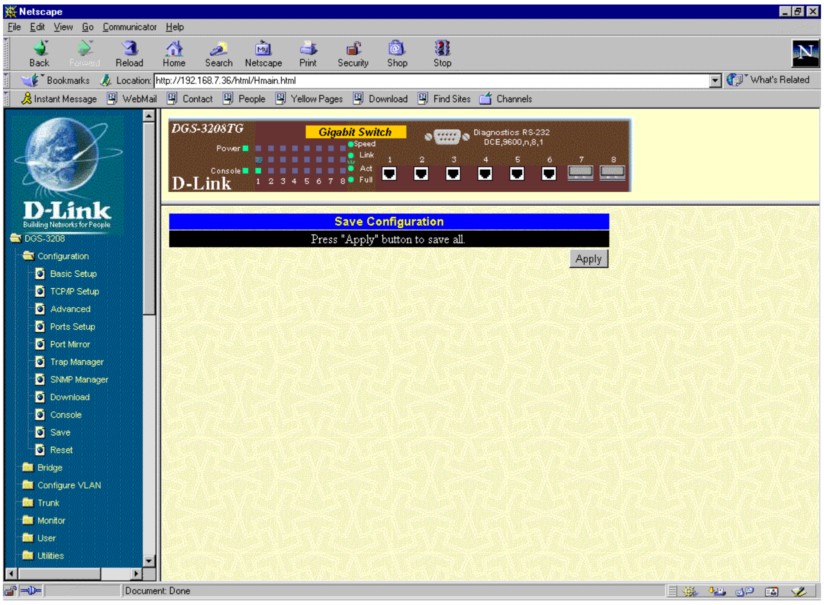
Parity=None

Stop Bits=1

The information is described as follows:

- **Console Timeout** Choose *Never*, *15 minutes*, *30 minutes*, *45 minutes*, or *60 minutes* for the desired refresh setting.
- **Serial Port** The options for the current console port setting are *Console* or *Slip*.
- **Baud Rate** Determines the serial port bit rate that will be used the next time the Switch is restarted. Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are 2400, 9600, 19200 and 38400 bits per second. The default setting in this Switch version is 9600.

## Save


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
D-Link
D-Link Building Networks for People
DGS-3208
Configuration
Basic Setup
TCP/IP Setup
Advanced
Ports Setup
Port Mirror
Trap Manager
SNMP Manager
Download
Console
Save
Reset
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Document: Done

Save Configuration

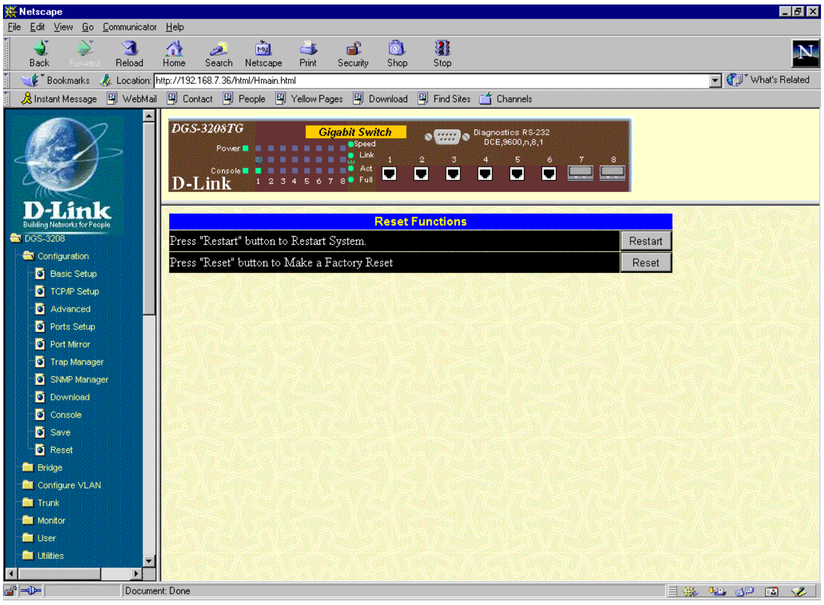
Press "Apply" button to save all.

Apply

**Figure 7-10. Save Configuration window**

To save all changes made in the current session to the Switch's flash memory, click the **Apply** button on this window.

## Reset


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
D-Link
D-Link Building Networks for People
DGS-3208
Configuration
Basic Setup
TCP/IP Setup
Advanced
Ports Setup
Port Mirror
Trap Manager
SNMP Manager
Download
Console
Save
Reset
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Document: Done

Reset Functions

Press "Restart" button to Restart System. Restart

Press "Reset" button to Make a Factory Reset Reset

**Figure 7-11. Reset Functions window**

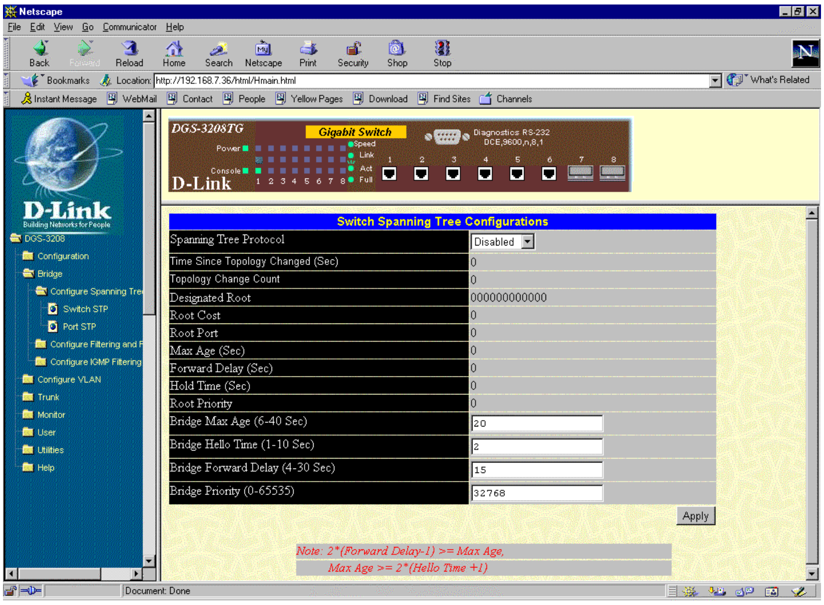
This window lets you restart the Switch or carry out a factory reset. Restarting the Switch clears transient data but preserves saved settings; a factory reset clears transient data and restores the settings that were in effect when the Switch left the factory.

# Bridge

This is the second category of the Web-based management program. The **Bridge** options include **Configure Spanning Tree Protocol** (**Switch STP** and **Port STP**), **Configure Filtering and Forwarding Table** (**Address Setup, Custom FDB**, **Filter Table**, and **Multicast FDB**), and **Configure IGMP Filtering** (**IGMP Setup** and, depending on the VLAN/MAC-based broadcast domain setting, **IGMP 802.1Q VLAN Setup** or **IGMP Port Based VLAN Setup**). See below for explanations of each one.

## Configure Spanning Tree Protocol

### *Switch STP*



Switch Spanning Tree Configurations

| | |
|---|---|
| Spanning Tree Protocol | Disabled |
| Time Since Topology Changed (Sec) | 0 |
| Topology Change Count | 0 |
| Designated Root | 000000000000 |
| Root Cost | 0 |
| Root Port | 0 |
| Max Age (Sec) | 0 |
| Forward Delay (Sec) | 0 |
| Hold Time (Sec) | 0 |
| Root Priority | 0 |
| Bridge Max Age (6-40 Sec) | 20 |
| Bridge Hello Time (1-10 Sec) | 2 |
| Bridge Forward Delay (4-30 Sec) | 15 |
| Bridge Priority (0-65535) | 32768 |

Apply

*Note: 2*(Forward Delay-1) >= Max Age,*
*Max Age >= 2*(Hello Time +1)*

**Figure 7-12. Switch Spanning Tree Configurations window**

The Switch supports the 801.2d Spanning Tree Protocol, which allows you to create alternative paths (with multiple switches or other types of bridges) in your network. See the Spanning Tree Algorithm section of the "*Switch Management Concepts*" chapter for a detailed explanation.

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

The information on the screen is described as follows:

- **Spanning Tree Protocol** Select *Enabled* to implement the Spanning Tree Protocol.
- **Time Since Topology Changes(sec)** Read-only object displays the last time changes were made to the network topology. These changes usually occur when backup paths are activated due to primary path failures.
- **Topology Change Count** Read-only object displays the number of times (since the current management session with the device was started) changes were made to the network topology. Changes usually occur on the network when backup paths are activated.
- **Designated Root** Read-only object displays the MAC (Ethernet) address of the bridge/switch on the network that has been chosen as the STP root.

- **Root Cost** Read-only object displays the cost for the path between the switch and the root bridge. If the switch is the root bridge, then the root cost is zero.

- **Root Port** Read-only object identifies the port (on the bridge) that offers the least path cost from the bridge to the root bridge. In the event of a network loop, data packets will pass through the root port.

- **Max Age(Sec)** Read-only object indicates the maximum age of STP information learned from the network (on any port) before it is discarded.

- **Forward Delay(sec)** Read-only object indicates how fast any port on the bridge can change its spanning state when moving towards the forwarding state. The value determines how long the port stays in each of the listening and learning states, which precede the forwarding state.

- **Hold Time(Sec)** Read-only object displays the time interval during which no more than two configuration BPDUs shall be transmitted by the bridge.

- **Root Priority(Sec)** Read-only object displays the priority number of the root bridge of the Spanning Tree. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multibridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. A bridge priority ranges from 0 to 65535, with 0 being the highest priority.

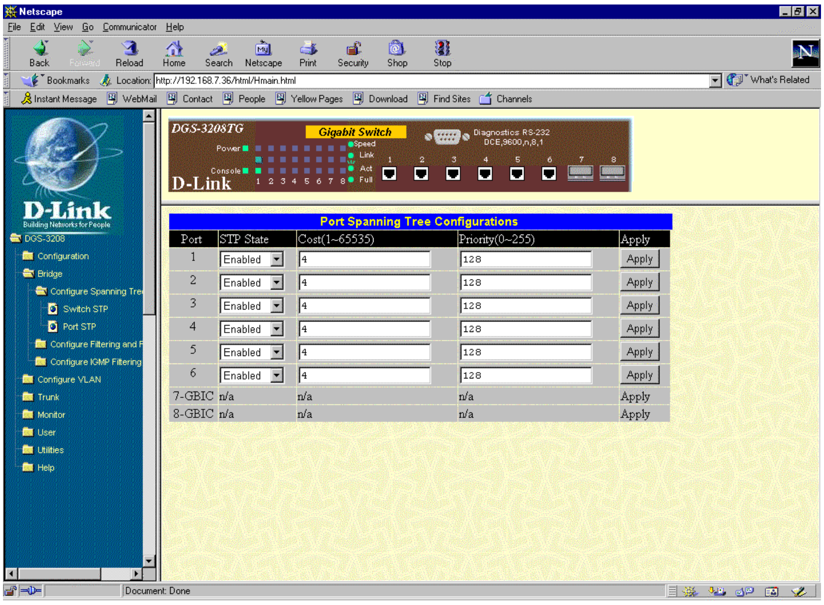
- **Bridge Max Age (6-40 Sec)** The Maximum Age is a read-write object that can be from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root ridge, your Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

- **Bridge Hello Time (1-10 Sec)** The Hello Time is a read-write object that can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

- **Bridge Forward Delay (4-30 Sec)** The Forward Delay is a read-write object that 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 (0-65535 Sec)** The Bridge Priority is a read-write object that can be from 0 to 65535. This is the priority number of the bridge. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multibridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. Zero is the highest priority.

### *Port STP*



Port Spanning Tree Configurations

| Port | STP State | Cost(1~65535) | Priority(0~255) | Apply |
|---|---|---|---|---|
| 1 | Enabled | 4 | 128 | Apply |
| 2 | Enabled | 4 | 128 | Apply |
| 3 | Enabled | 4 | 128 | Apply |
| 4 | Enabled | 4 | 128 | Apply |
| 5 | Enabled | 4 | 128 | Apply |
| 6 | Enabled | 4 | 128 | Apply |
| 7-GBIC | n/a | n/a | n/a | Apply |
| 8-GBIC | n/a | n/a | n/a | Apply |

**Figure 7-13. Port Spanning Tree Configurations window**

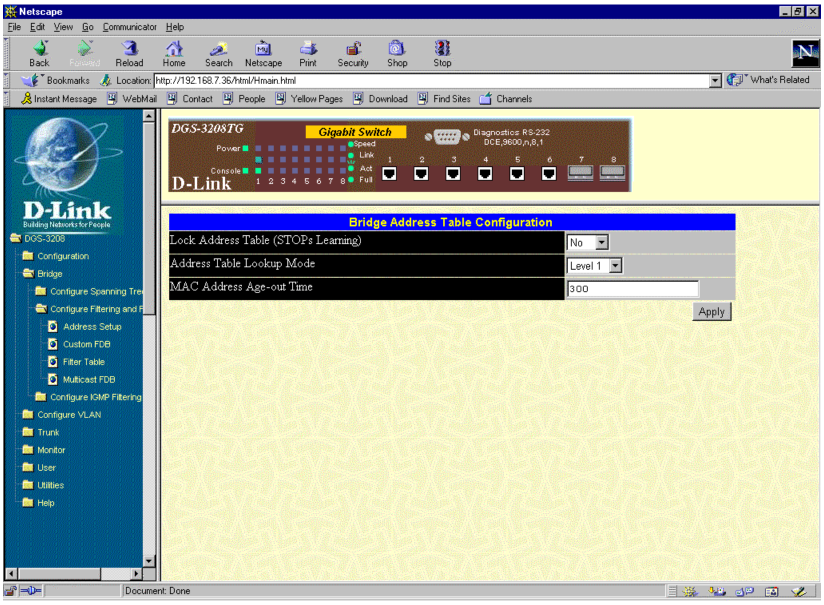
The information on the window is described as follows:

- **STP State** The Spanning Tree Protocol state for a selected port can either be *Enabled* or *Disabled*.
- **Cost(1~65535)** The Path Cost is a changeable parameter and may be modified according to the Spanning Tree Algorithm specification.
- **Priority(0~255)** The read-write object displays the priority number of the port. The value is used in conjunction with the physical port number to set the port ID, which in turn is used when determining the root port of the bridge. The smaller the number set, the higher the port priority is. The higher the port priority, the more chances the port has of becoming the root port. Port priority ranges from 0 to 255, with 0 being the highest port priority.

## Configure Filtering and Forwarding Table

### *Address Setup*

The **Address Setup** window lets you stop or restart MAC address learning, adjust address table size, and control how long learned addresses are retained in the table.



Location: http://192.168.7.36/html/Hmain.html

| Bridge Address Table Configuration | |
|---|---|
| Lock Address Table (STOPs Learning) | No |
| Address Table Lookup Mode | Level 1 |
| MAC Address Age-out Time | 300 |

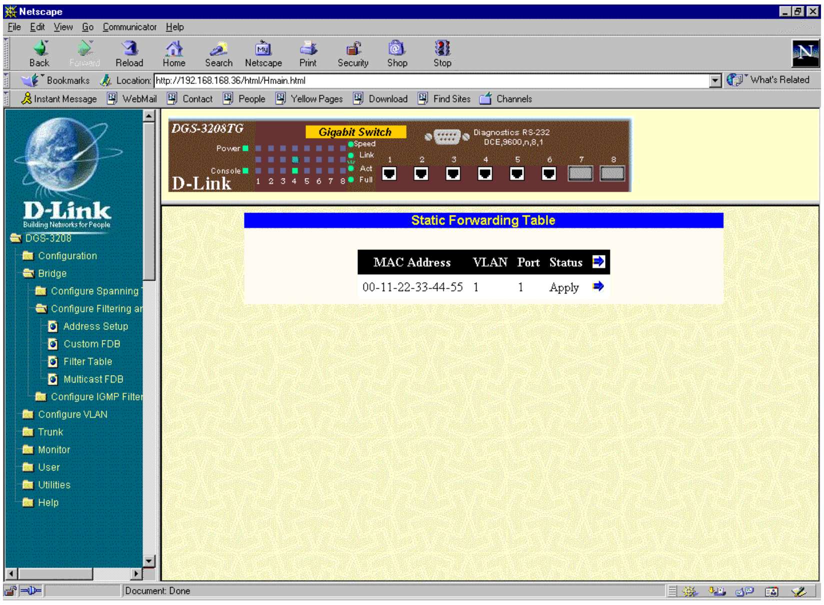
Figure 7-14.  Bridge Address Table Configurations window

- ♦ **Lock Address Table(STOPs Learning)** This function is used mostly for security purposes. When the forwarding table is locked, the Switch will no longer learn the MAC addresses for new hosts. If your network configuration doesn't change, locking the forwarding table helps keep intruders off your network, since any packet coming from an unknown source address will be dropped by the Switch.

- ♦ **Address Table Lookup Mode** This setting allows the user to tailor the MAC address look-up procedure. Choices are *Level 0*, *Level 1*, *Level 2*, *Level 3*, *Level 4*, *Level 5*, *Level 6*, and *Level 7*. The higher the level, the more MAC addresses can be learned by the Switch. However, a side effect is that throughput will be degraded the higher the level you select. This setting will take effect after your system reboots.

- ♦ **MAC Address Age-out Time** Enter the desired MAC address age-out time in this field (1 to 9999 minutes) .

## *Custom FDB*



Location: http://192.168.168.36/html/Hmain.html

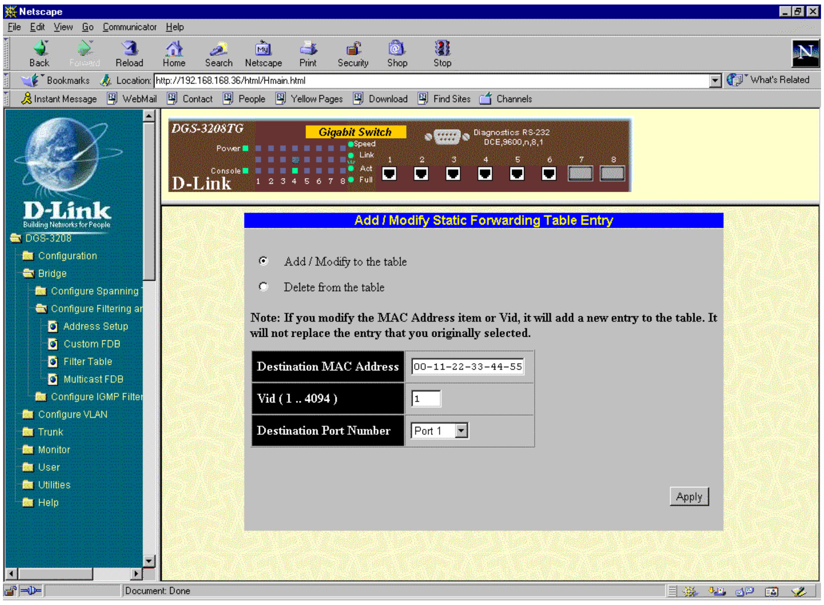
Static Forwarding Table

| MAC Address | VLAN | Port | Status |
|---|---|---|---|
| 00-11-22-33-44-55 | 1 | 1 | Apply |

Figure 7-15.  Static Forwarding Table window

MAC forwarding allows the Switch to permanently forward outbound traffic to specific destination MAC addresses over a specified port. You can also use this feature to restrict inbound traffic based on source MAC addresses.

Click the arrow icon on the window above to add or modify static forwarding table entries. The following window appears:



Add / Modify Static Forwarding Table Entry

● Add / Modify to the table

○ Delete from the table

Note: If you modify the MAC Address item or Vid, it will add a new entry to the table. It will not replace the entry that you originally selected.

| | |
|---|---|
| Destination MAC Address | 00-11-22-33-44-55 |
| Vid ( 1 .. 4094 ) | 1 |
| Destination Port Number | Port 1 |

Apply

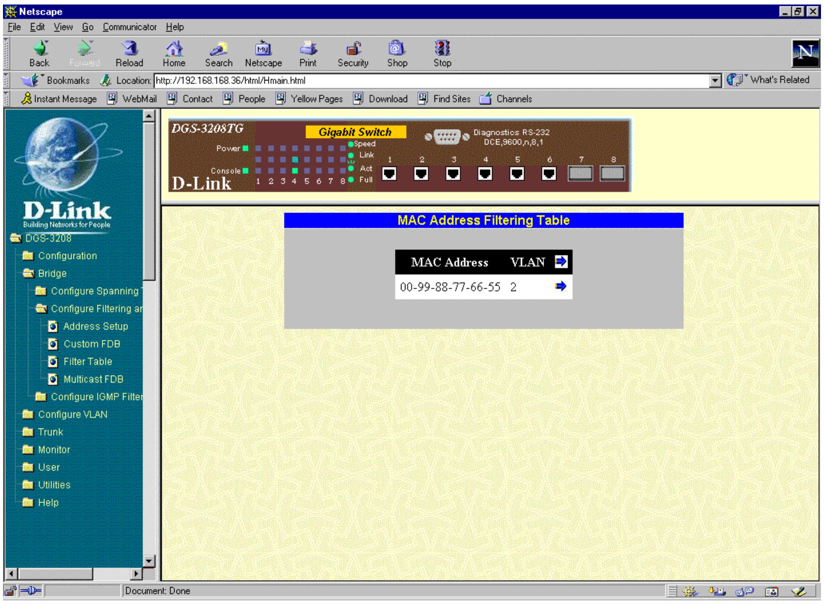
Figure 7-16. Add / Modify Static Forwarding Table Entry window

To use the MAC forwarding function, enter the MAC address of the device to which the specified port permanently forwards traffic in the destination MAC Address field, enter a VLAN ID (if applicable), and enter the port number that permanently forwards traffic from the specified device in the destination port number field. Then click **Apply** to let your changes take effect.

The information in the screen is described as follows:

- **Destination MAC Address** The MAC address of the device to which the specified port permanently forwards traffic.
- **Vid(1..4094)** Enter a VLAN ID number between 1 and 4094.
- **Destination Port Number** The port number that permanently forwards traffic from the specified device, regardless of the device's network activity or current network congestion.

### *Filter Table*



MAC Address Filtering Table

| MAC Address | VLAN |
|---|---|
| 00-99-88-77-66-55 | 2 |

**Figure 7-17. MAC Address Filtering Table window**

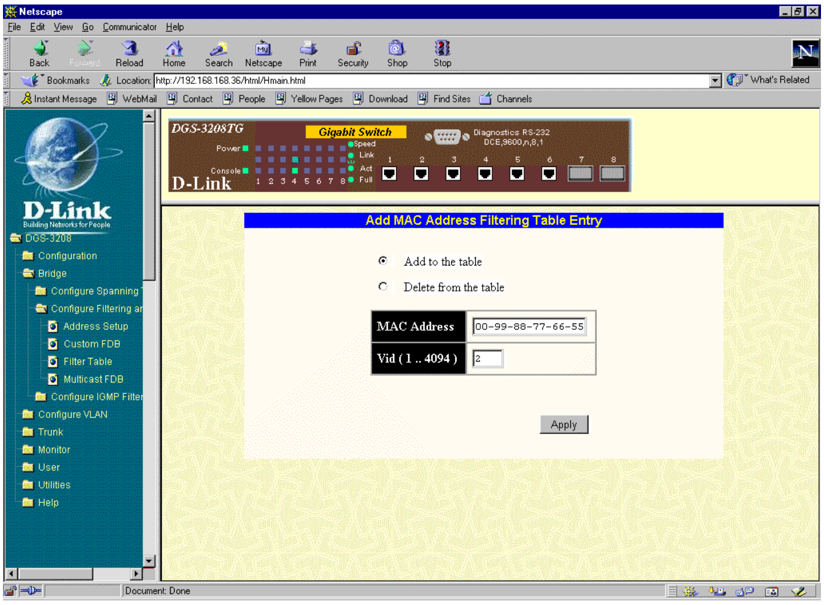
MAC filtering allows the Switch to block inbound traffic from unknown or unwanted devices by mapping a port to a source MAC address.

To use the MAC filtering function, enter the MAC address of the device allowed to send traffic in the MAC Address field and select the desired setting in the Filter Status field. Then click **Apply**.

The information in the window is described as follows:

- **MAC Address** The Ethernet address of the MAC filtering table entry.
- **VLAN** The VLAN ID number of the MAC filtering table entry.

Click the arrow icon to access the **Add MAC Address Filtering Table Entry** window:


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.168.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure Spanning
Configure Filtering ar
Address Setup
Custom FDB
Filter Table
Multicast FDB
Configure IGMP Filter
Configure VLAN
Trunk
Monitor
User
Utilities
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
Document: Done

Add MAC Address Filtering Table Entry

● Add to the table

○ Delete from the table

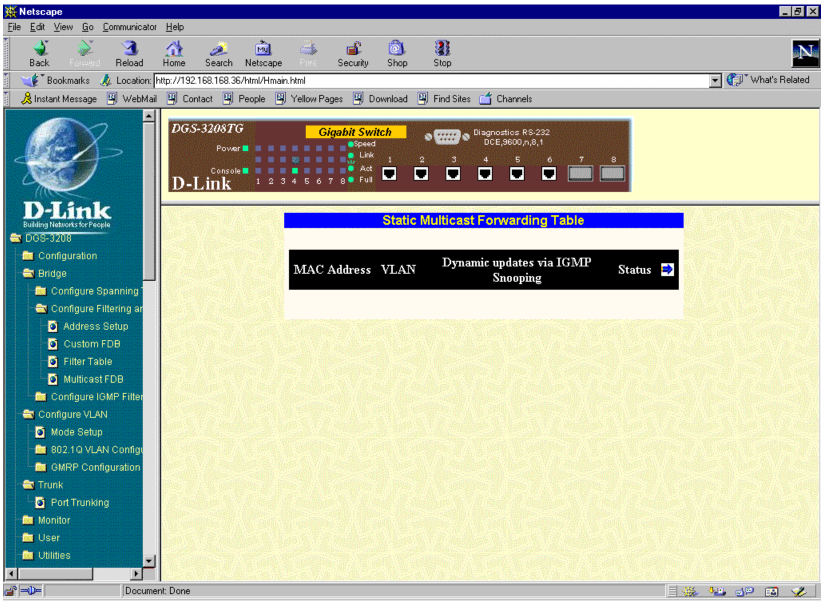
| | |
|---|---|
| MAC Address | 00-99-88-77-66-55 |
| Vid ( 1 .. 4094 ) | 2 |

Apply

Figure 7-18. Add MAC Address Filtering Table Entry window

To use the static filtering function, enter the MAC address of the device allowed to send traffic in the MAC Address field, enter a VLAN ID, and then click **Apply**.

### *Multicast FDB*



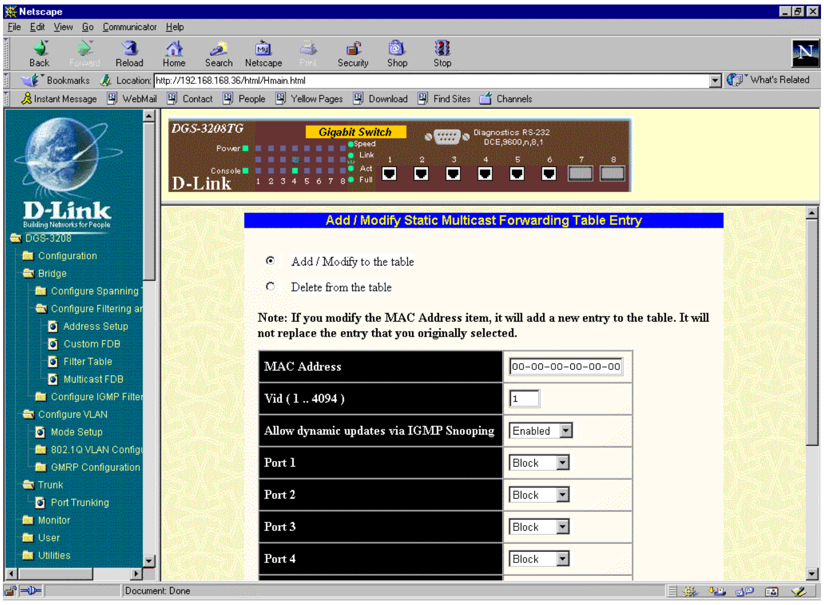
Static Multicast Forwarding Table

| MAC Address | VLAN | Dynamic updates via IGMP Snooping | Status |
|---|---|---|---|

Figure 7-19. Static Multicast Forwarding Table window

This window allows you to forward or block traffic over each port for one multicast group.

Click the arrow icon to access the **Add / Modify Static Multicast Forwarding Table Entry** window:



**Add / Modify Static Multicast Forwarding Table Entry**

● Add / Modify to the table

○ Delete from the table

Note: If you modify the MAC Address item, it will add a new entry to the table. It will not replace the entry that you originally selected.

| | |
|---|---|
| MAC Address | 00-00-00-00-00-00 |
| Vid ( 1 .. 4094 ) | 1 |
| Allow dynamic updates via IGMP Snooping | Enabled |
| Port 1 | Block |
| Port 2 | Block |
| Port 3 | Block |
| Port 4 | Block |

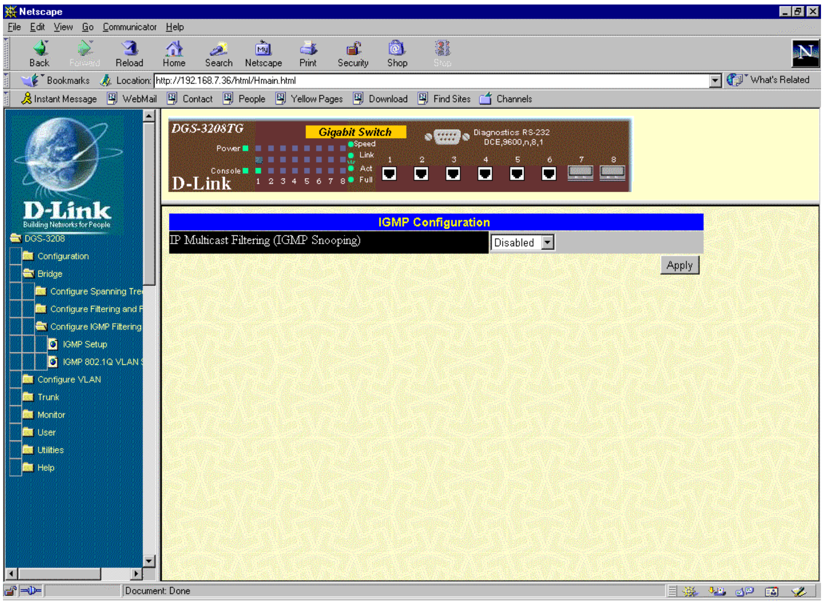
Figure 7-20. Add / Modify Static Multicast Forwarding Table Entry window

To edit or create a new filter, enter the desired MAC address as well as the VLAN ID number in the first two fields, respectively. Next, enable or disable dynamic updates via IGMP Snooping. Finally, toggle each desired port to *Forward* or *Block*. Click **Apply** to activate the filter.

## Configure IGMP Filtering

### *IGMP Setup*

The IGMP Setup command lets you check and adjust Internet Group Management Protocol settings, which affect handling of IP multicast packets.



**IGMP Configuration**

| | |
|---|---|
| IP Multicast Filtering (IGMP Snooping) | Disabled |

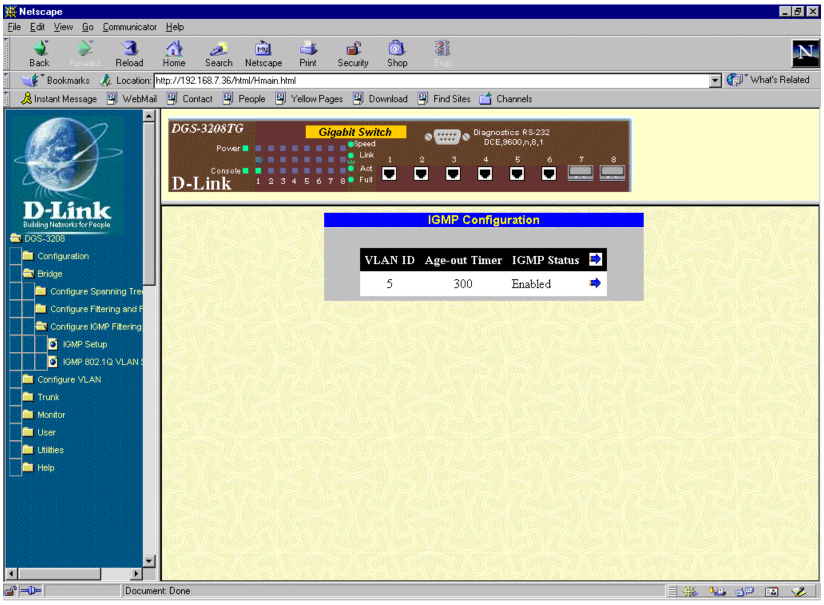
Apply

Figure 7-21. first IGMP Configuration window

- **IP Multicast Filtering (IGMP Snooping)** This enables or disables the Switch to intelligently forward IGMP and multicast packets instead of broadcasting (flooding) them on all ports. This setting also enables

IGMP snooping, which enables the Switch to read IGMP packets being forwarded through the Switch in order to obtain forwarding information from them (learn which ports contain multicast members).

## *IGMP 802.1Q VLAN Setup*


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure Spanning Tre
Configure Filtering and F
Configure IGMP Filtering
IGMP Setup
IGMP 802.1Q VLAN S
Configure VLAN
Trunk
Monitor
User
Utilities
Help
DGS-3208TG
Gigabit Switch
D-Link
Document: Done

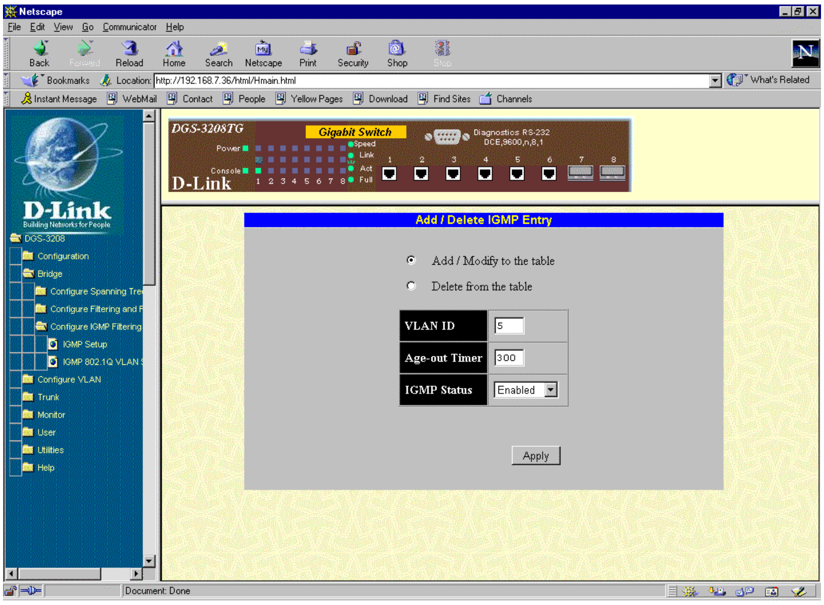
IGMP Configuration

| VLAN ID | Age-out Timer | IGMP Status | |
|---|---|---|---|
| 5 | 300 | Enabled | ➡ |

Figure 7-22. second IGMP Configuration window

This table displays IGMP configuration information.

Click the arrow icon to access the **Add / Delete IGMP Entry** window:


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure Spanning Tre
Configure Filtering and F
Configure IGMP Filtering
IGMP Setup
IGMP 802.1Q VLAN S
Configure VLAN
Trunk
Monitor
User
Utilities
Help
DGS-3208TG
Gigabit Switch
D-Link
Document: Done

Add / Delete IGMP Entry

● Add / Modify to the table

○ Delete from the table

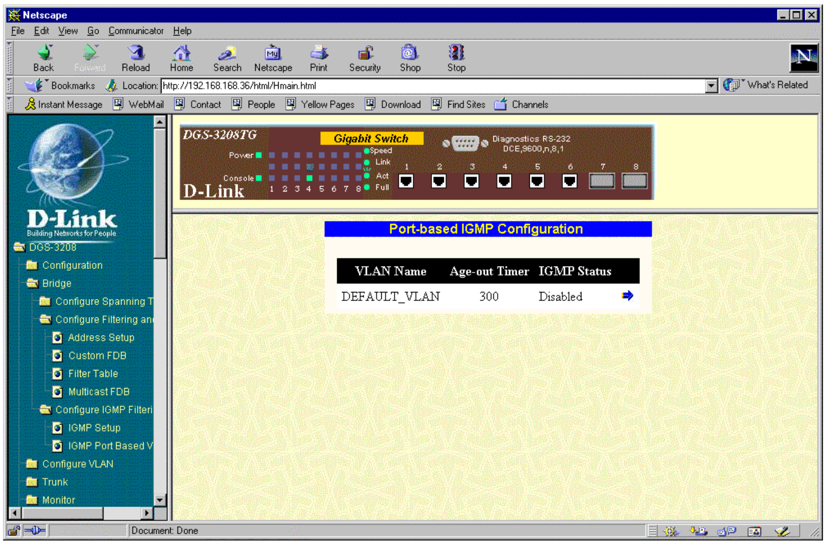
| | |
|---|---|
| VLAN ID | 5 |
| Age-out Timer | 300 |
| IGMP Status | Enabled |

Apply

Figure 7-23. Add / Delete IGMP Entry window

Enter a VLAN ID number in the first field, enter an IGMP entry aging time in the next field, disable or enable IGMP status, and click **Apply** to let your changes take effect.

### *IGMP Port Based VLAN Setup*


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.168.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure Spanning T
Configure Filtering an
Address Setup
Custom FDB
Filter Table
Multicast FDB
Configure IGMP Filteri
IGMP Setup
IGMP Port Based V
Configure VLAN
Trunk
Monitor
DGS-3208TG
Gigabit Switch
Document: Done

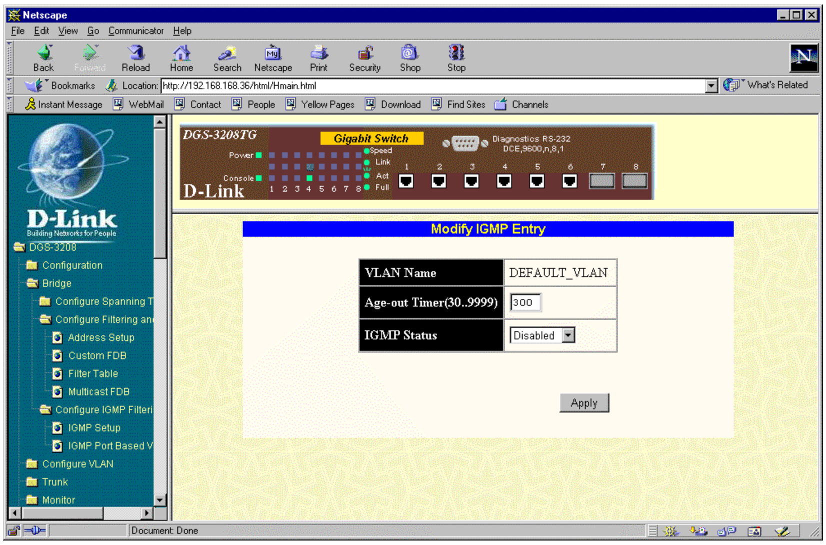
Port-based IGMP Configuration

| VLAN Name | Age-out Timer | IGMP Status | |
|---|---|---|---|
| DEFAULT_VLAN | 300 | Disabled | ➡ |

**Figure 7-24. Port-based IGMP Configuration window**

This table displays IGMP configuration information.

Click the arrow icon to access the **Modify IGMP Entry** window:


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.168.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure Spanning T
Configure Filtering an
Address Setup
Custom FDB
Filter Table
Multicast FDB
Configure IGMP Filteri
IGMP Setup
IGMP Port Based V
Configure VLAN
Trunk
Monitor
DGS-3208TG
Gigabit Switch
Document: Done

Modify IGMP Entry

| | |
|---|---|
| VLAN Name | DEFAULT_VLAN |
| Age-out Timer(30..9999) | 300 |
| IGMP Status | Disabled |

Apply

**Figure 7-25. Modify IGMP Entry window**

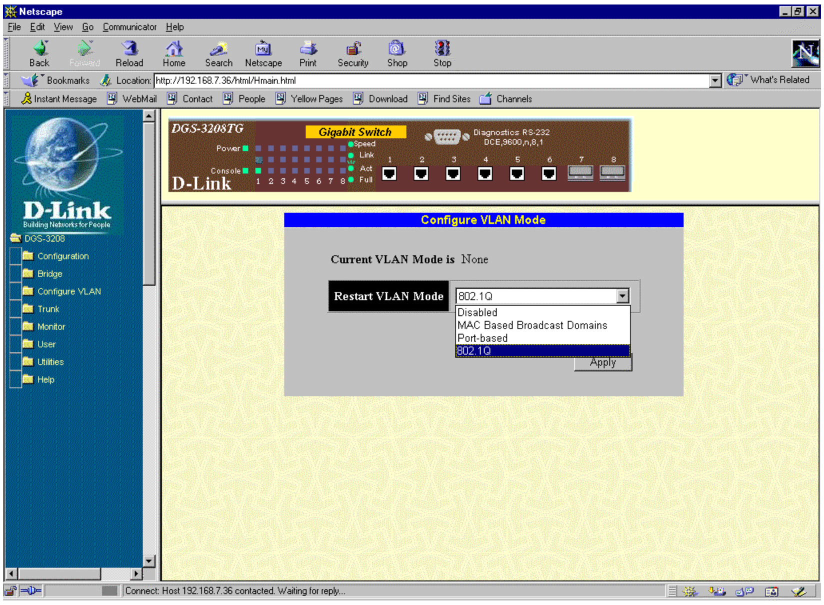
Enter a VLAN ID name in the first field, enter an IGMP entry aging time in the next field, disable or enable IGMP status, and click **Apply** to let your changes take effect.

# *Configure VLAN*

This is the third category of the Web-based management program. The **Configure VLAN** options depend on which VLAN or MAC-based broadcast domain mode you are in. **Mode Setup** and **MAC-based** are the main screens for MAC-based broadcast domains. **Mode Setup** and **Port based VLAN Setup** are the main screens for port-based VLANs. **Mode Setup**, **802.1Q VLAN Configuration** (**Port VID Setup**, **Ingress Filtering Check**, **802.1Q VLAN Setup**, **GVRP Configuration**, and **GMRP Configuration**) and **GMRP Configuration** (**Device GMRP Configuration** and **802.1Q VLAN Multicast FDB**) are the main screens for 802.1Q VLANs.

Please note that if you are unsure about this material, we highly recommend consulting Chapter 5, "*Switch Management Concepts.*"

## Mode Setup


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232
DCE,9600,n,8,1
Power
Console
Speed
Link
Act
Full
1 2 3 4 5 6 7 8
D-Link

Configure VLAN Mode

Current VLAN Mode is None

Restart VLAN Mode 802.1Q

Disabled
MAC Based Broadcast Domains
Port-based
802.1Q

Apply

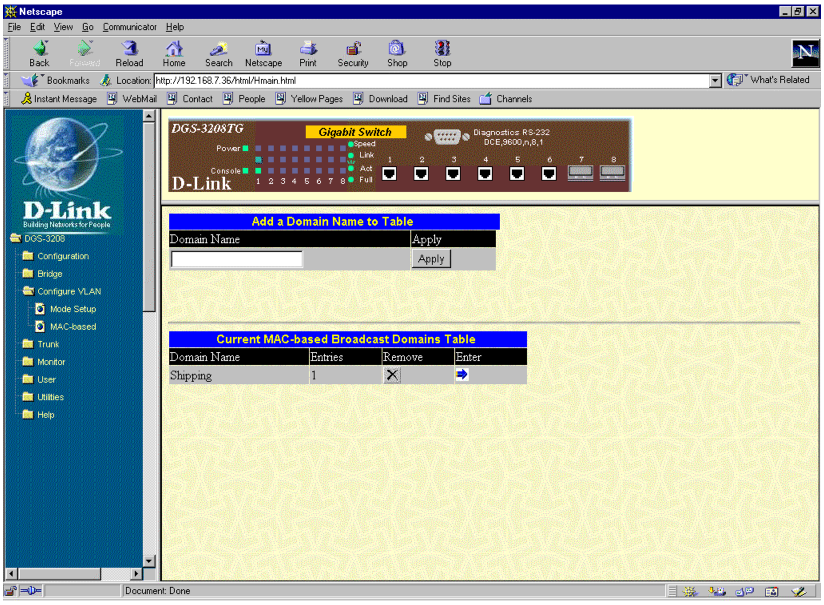
Connect: Host 192.168.7.36 contacted. Waiting for reply...

**Figure 7-26. Configure VLAN Mode window**

To use one of these three modes, select *MAC Based Broadcast Domains*, *802.1Q* or *Port-based* under Restart VLAN Mode**--**otherwise, leave the setting at *Disabled*. Then click **Apply** and reboot the Switch.

## Mac-based

A MAC-based broadcast domain is a collection of users or ports grouped together for the purpose of secure, autonomous broadcasting and multicasting. Members of a MAC-based broadcast domain must all be directly connected to the Switch. The Switch supports up to twelve MAC-based broadcast domains.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Location: http://192.168.7.36/html/Hmain.html
DGS-3208TG
Gigabit Switch
D-Link
DGS-3208
Configuration
Bridge
Configure VLAN
Mode Setup
MAC-based
Trunk
Monitor
User
Utilities
Help
Document: Done

**Add a Domain Name to Table**

| Domain Name | Apply |
|---|---|
| | Apply |

**Current MAC-based Broadcast Domains Table**

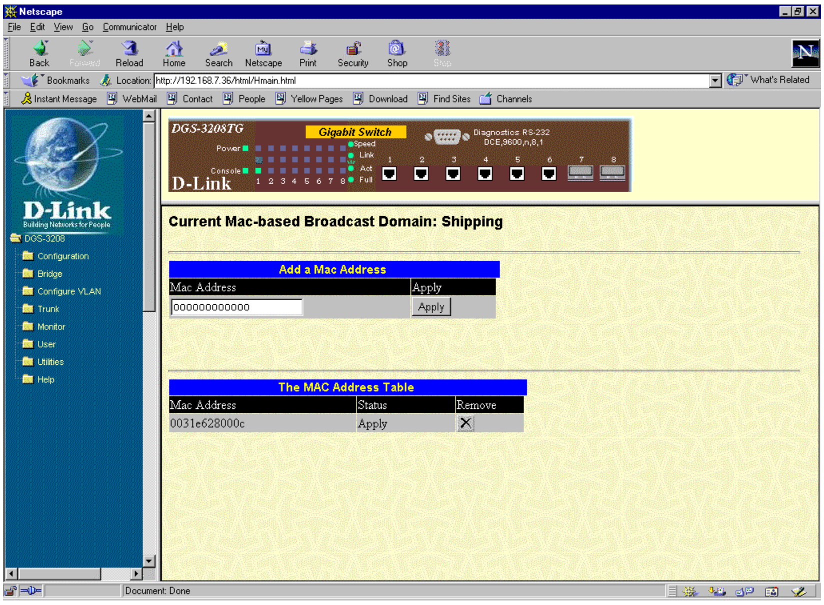
| Domain Name | Entries | Remove | Enter |
|---|---|---|---|
| Shipping | 1 | ☒ | → |

Figure 7-27. Add a Domain Name to Table window

This window lets you create and remove MAC-based broadcast domains. In the Domain Name field, which is initially blank, type the name or number that you wish to give the domain; then click **Apply** to add the name to the table.

You can click the button under Remove to delete a domain.

Click the arrow under Enter to add entries to this table. The following window appears:


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Location: http://192.168.7.36/html/Hmain.html
DGS-3208TG
Gigabit Switch
D-Link
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Help
Document: Done

**Current Mac-based Broadcast Domain: Shipping**

**Add a Mac Address**

| Mac Address | Apply |
|---|---|
| 000000000000 | Apply |

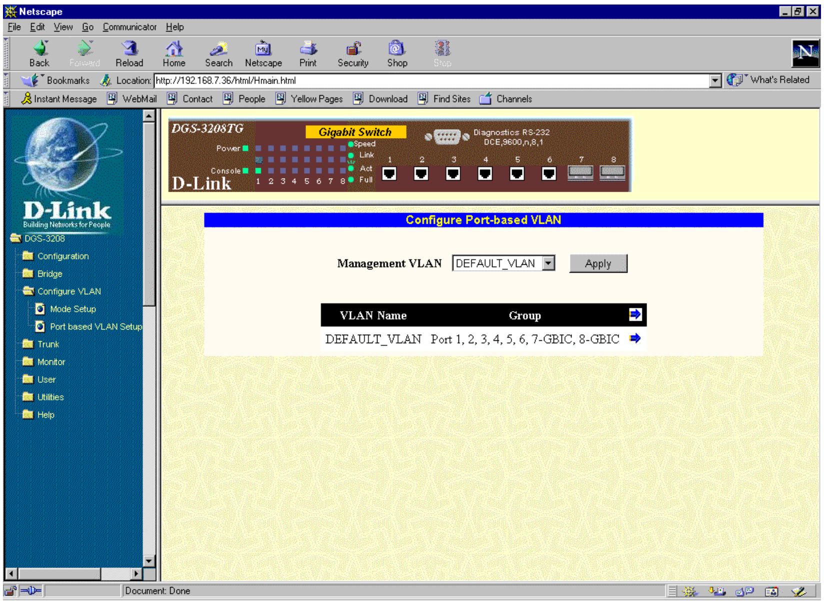
**The MAC Address Table**

| Mac Address | Status | Remove |
|---|---|---|
| 0031e628000c | Apply | ☒ |

Figure 7-28. Add a Mac Address window

This window lets you designate particular machines on your network as members of the MAC-based broadcast domain named in the title above. To add a machine to the domain, enter the machine's MAC address and click **Apply**. The address will appear in the table in the lower part of the screen. You can then view its status (which depends on whether the setting has been saved and the Switch restarted) or, if you wish, remove it by clicking the button under **Remove**.

## Port Based VLAN Setup


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
D-Link
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Mode Setup
Port based VLAN Setup
Trunk
Monitor
User
Utilities
Help
Document: Done

Configure Port-based VLAN

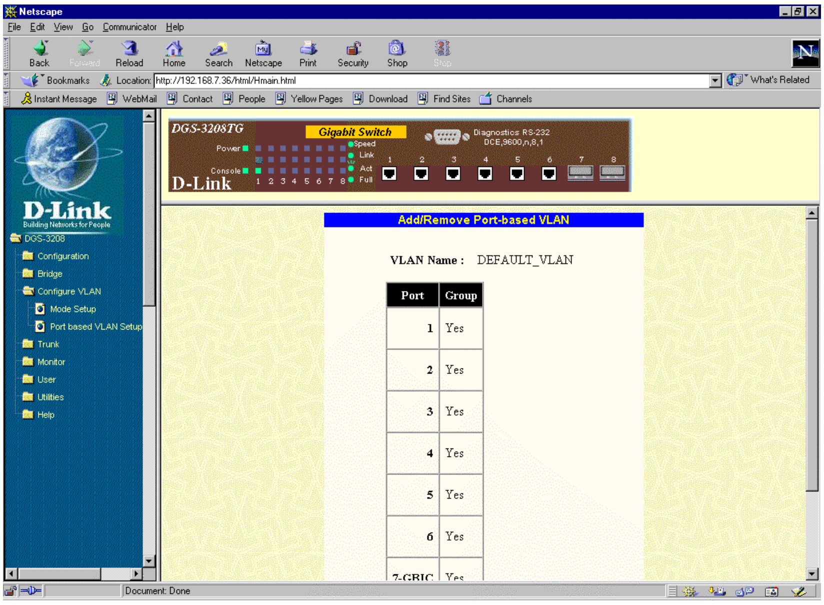
Management VLAN: DEFAULT_VLAN — Apply

| VLAN Name | Group |
|---|---|
| DEFAULT_VLAN | Port 1, 2, 3, 4, 5, 6, 7-GBIC, 8-GBIC |

Figure 7-29. Configure Port-based VLAN window

Select a management VLAN at the top of the window and then click **Apply**.

Click the pointer icon on the far right on the window above to access the **Add/Remove Port-based VLAN** window:


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
D-Link
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Mode Setup
Port based VLAN Setup
Trunk
Monitor
User
Utilities
Help
Document: Done

Add/Remove Port-based VLAN

VLAN Name : DEFAULT_VLAN

| Port | Group |
|---|---|
| 1 | Yes |
| 2 | Yes |
| 3 | Yes |
| 4 | Yes |
| 5 | Yes |
| 6 | Yes |
| 7-GBIC | Yes |

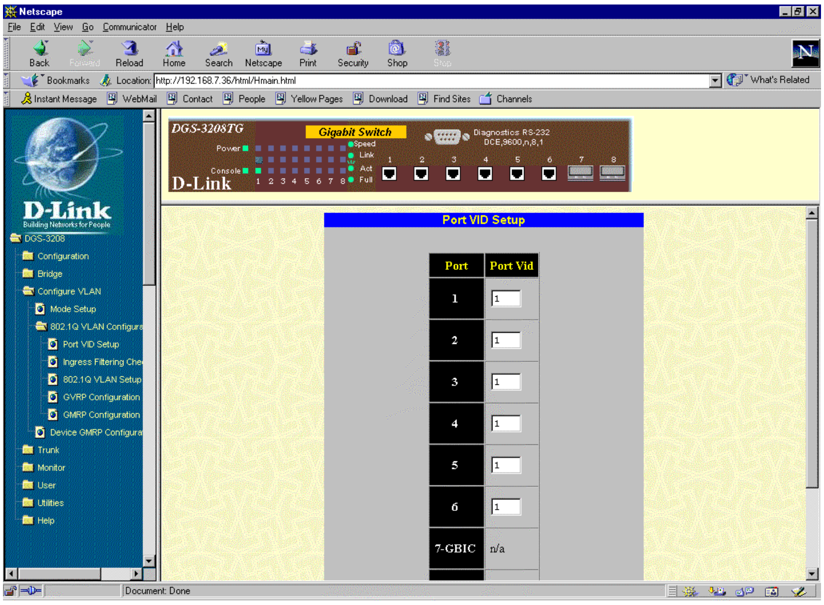
Figure 7-30. Add/Remove Port-based VLAN window

To delete a port-based VLAN, select Delete from the table, change each port's Group setting to *No*, and then click **Apply** to let your change take effect.

To make a change to a port-based VLAN, select Modify to the table and then make the desired changes to the Group settings. Click **Apply** to let your changes take effect.

## 802.1Q VLAN Configuration

### *Port VID Setup*



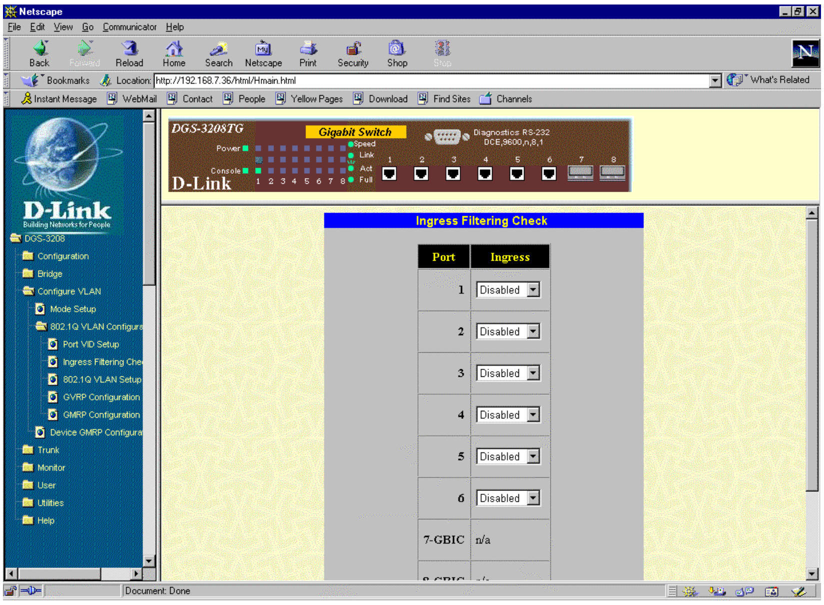
Port VID Setup

| Port | Port Vid |
|---|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |
| 4 | 1 |
| 5 | 1 |
| 6 | 1 |
| 7-GBIC | n/a |

**Figure 7-31. Port VID Setup window**

Use this window to assign a default VLAN ID for each desired port. Click **Apply** to let the settings take effect.

### *Ingress Filtering Check*



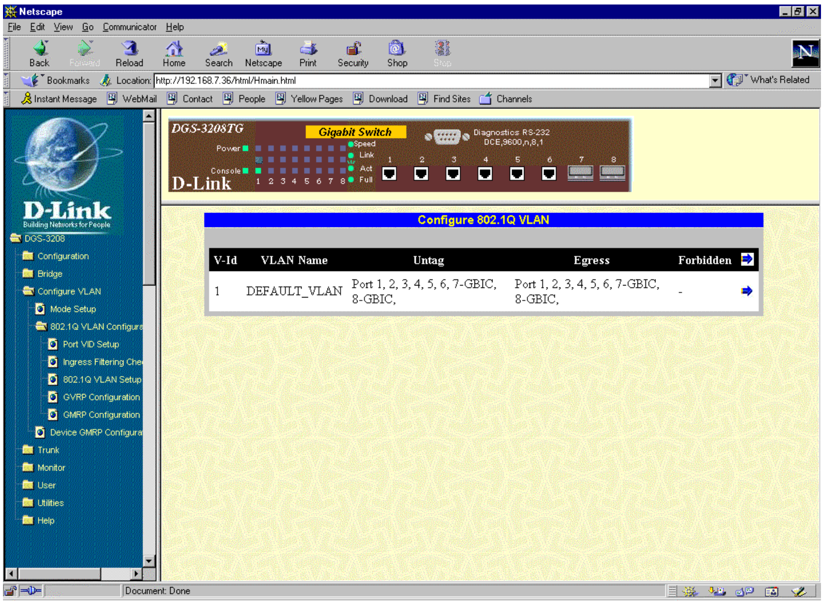
Ingress Filtering Check

| Port | Ingress |
|---|---|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |
| 6 | Disabled |
| 7-GBIC | n/a |

**Figure 7-32. Ingress Filtering Check window**

Use this window to enable or disable the ingress filtering check for each desired port. Ingress filtering means that a receiving port will check to see if it is a member of the VLAN ID in the packet before forwarding the packet. Click **Apply** to let the settings take effect.

### *802.1Q VLAN Setup*



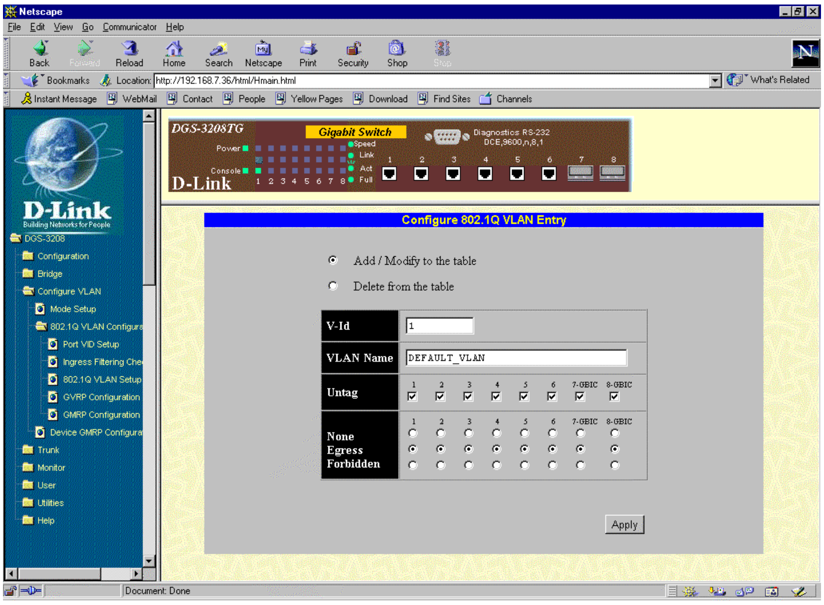
Configure 802.1Q VLAN

| V-Id | VLAN Name | Untag | Egress | Forbidden |
|---|---|---|---|---|
| 1 | DEFAULT_VLAN | Port 1, 2, 3, 4, 5, 6, 7-GBIC, 8-GBIC, | Port 1, 2, 3, 4, 5, 6, 7-GBIC, 8-GBIC, | - |

**Figure 7-33. Configure 802.1Q VLAN window**

Click the **X** in the Delete column next to an entry to remove it from the table.

Click the pointer icon to access the Configure **802.1Q VLAN Entry** window:



Configure 802.1Q VLAN Entry

● Add / Modify to the table

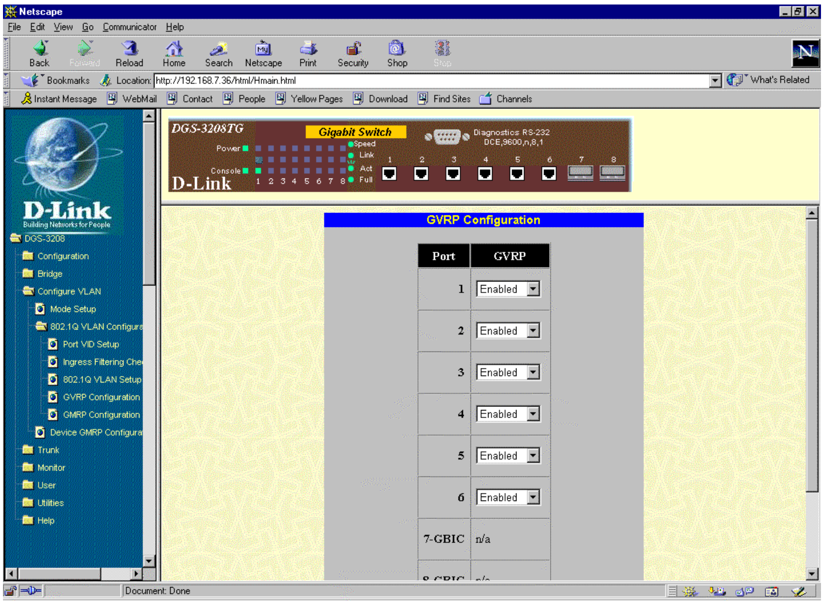
○ Delete from the table

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| V-Id | 1 |  |  |  |  |  |  |  |
| VLAN Name | DEFAULT_VLAN |  |  |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7-GBIC | 8-GBIC |
| Untag | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7-GBIC | 8-GBIC |
| None | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Egress | ● | ● | ● | ● | ● | ● | ● | ● |
| Forbidden | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

**Figure 7-34. Configure 802.1Q VLAN Entry window**

To configure an 802.1Q VLAN entry, enter a VLAN ID number and VLAN Name in the first two fields. Next, check *Untag* for each member port that is not a tagging port. *None* should be checked if you don't want a port to belong to a VLAN. Check *Egress* to statically set a port to belong to a VLAN. Checking *Forbidden* prevents the port from joining a VLAN dynamically as well as defining the port as a non-member. Click **Apply** to let the changes take effect.

## *GVRP Configuration*


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Mode Setup
802.1Q VLAN Configura
Port VID Setup
Ingress Filtering Che
802.1Q VLAN Setup
GVRP Configuration
GMRP Configuration
Device GMRP Configura
Trunk
Monitor
User
Utilities
Help
DGS-3208TG Gigabit Switch
Power Console Speed Link Act Full
Diagnostics RS-232 DCE,9600,n,8,1
D-Link
Document: Done

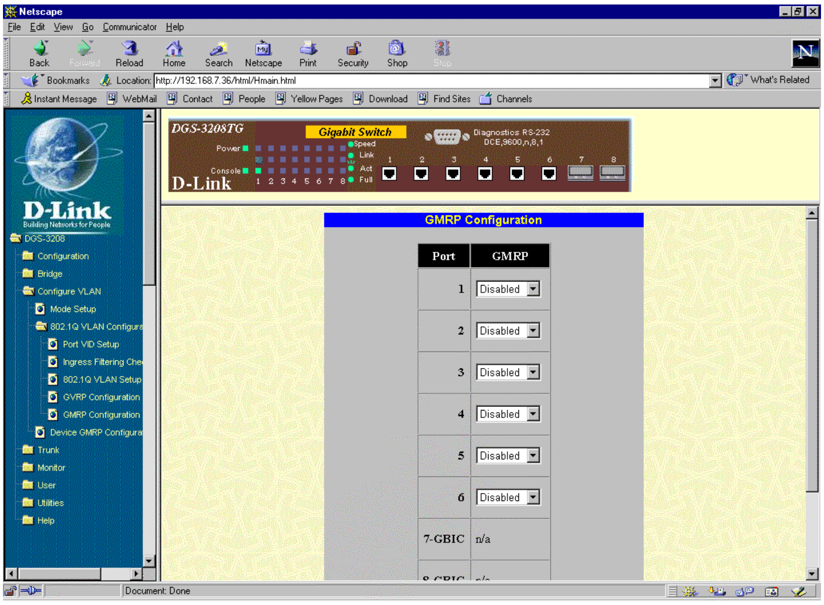
GVRP Configuration

| Port | GVRP |
|---|---|
| 1 | Enabled |
| 2 | Enabled |
| 3 | Enabled |
| 4 | Enabled |
| 5 | Enabled |
| 6 | Enabled |
| 7-GBIC | n/a |
| 8-GBIC | n/a |

**Figure 7-35. GVRP Configuration window**

Use this window to enable or disable GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol, for each desired port. Click **Apply** to let the settings take effect.

## *GMRP Configuration*


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Mode Setup
802.1Q VLAN Configura
Port VID Setup
Ingress Filtering Che
802.1Q VLAN Setup
GVRP Configuration
GMRP Configuration
Device GMRP Configura
Trunk
Monitor
User
Utilities
Help
DGS-3208TG Gigabit Switch
Power Console Speed Link Act Full
Diagnostics RS-232 DCE,9600,n,8,1
D-Link
Document: Done

GMRP Configuration

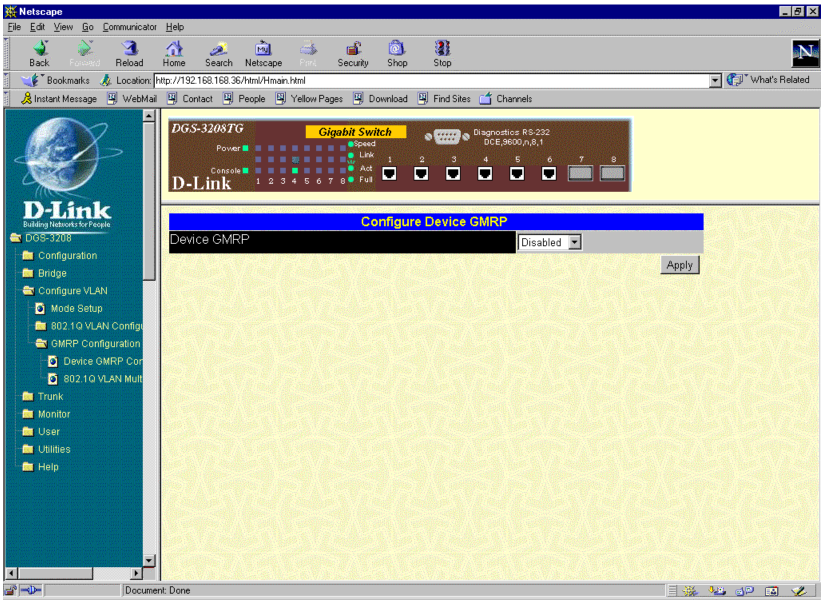
| Port | GMRP |
|---|---|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |
| 6 | Disabled |
| 7-GBIC | n/a |
| 8-GBIC | n/a |

**Figure 7-36. GMRP Configuration window**

Use this window to disable or enable Group Multicast Registration Protocol (GMRP) on individual ports on the Switch. Click **Apply** to let the change take effect.

## GMRP Configuration

### *Device GMRP Configuration*



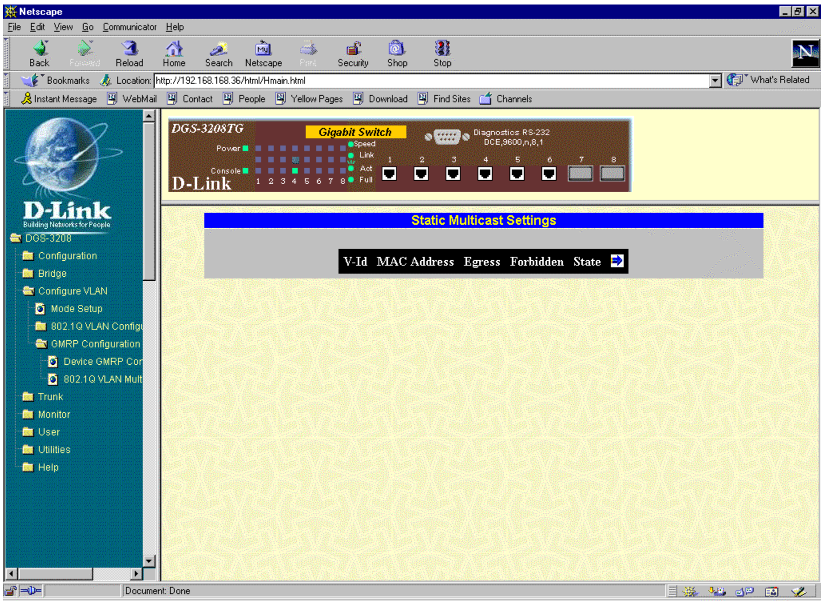
Configure Device GMRP

Device GMRP: Disabled

**Figure 7-37. Configure Device GMRP window**

Use this window to enable or disable Group Multicast Registration Protocol (GMRP) on the Switch. Click **Apply** to let your change take effect.

### *802.1Q VLAN Multicast FDB*



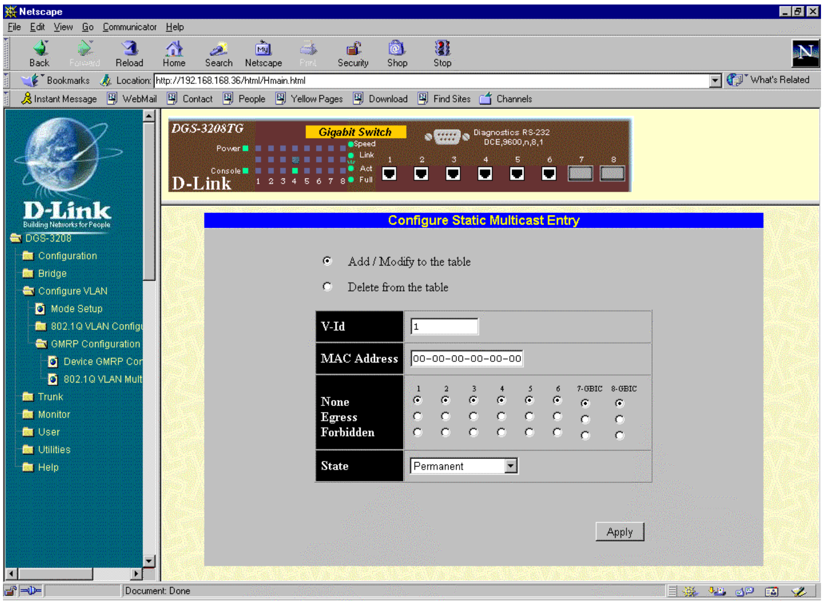
Static Multicast Settings

| V-Id | MAC Address | Egress | Forbidden | State |
|---|---|---|---|---|

**Figure 7-38. Static Multicast Settings window**

This window allows you to forward traffic over each port for one multicast group.

Click the arrow icon to access the **Configure Static Multicast Entry** window:



Configure Static Multicast Entry

● Add / Modify to the table

○ Delete from the table

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| V-Id | 1 | | | | | | | |
| MAC Address | 00-00-00-00-00-00 | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7-GBIC | 8-GBIC |
| None | ● | ● | ● | ● | ● | ● | ● | ● |
| Egress | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Forbidden | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| State | Permanent | | | | | | | |

Apply

**Figure 7-39. Configure Static Multicast Entry window**

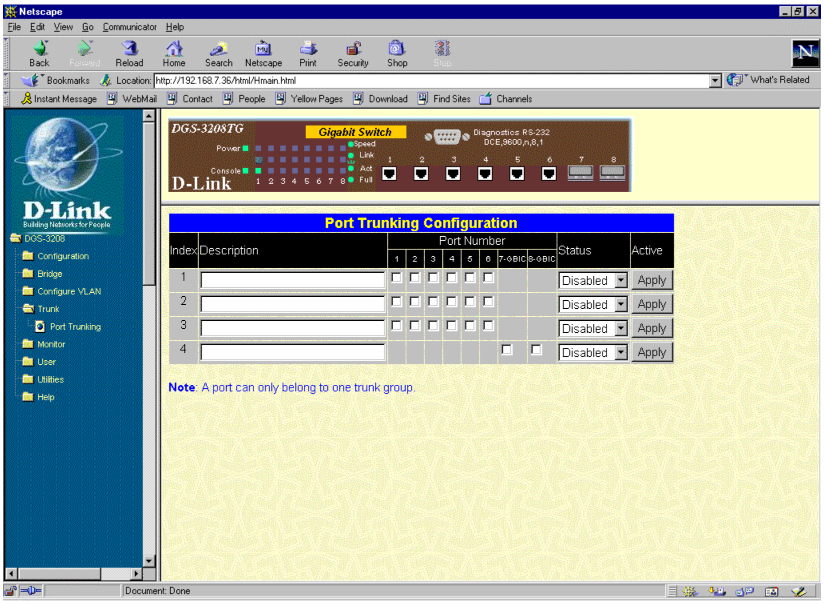
To edit or create a new filter, enter the desired VLAN ID number as well as the MAC address in the first two fields, respectively. Next, check either *None*, *Egress*, or *Forbidden* for each port. *None* should be checked if you don't want a port to belong to a VLAN. Check *Egress* to statically set a port to belong to a VLAN. Checking *Forbidden* prevents the port from joining a VLAN dynamically as well as defining the port as a non-member. Select the appropriate State (*Permanent*, *Delete on Reset*, *Delete on Timeout*, or *Invalid*). Click **Apply** to activate the filter.

## *Trunk*

This is the fourth category of the Web-based management program. One item is featured in this section, **Port Trunking**.

Port trunking is used to combine a number of ports together to make a single high-bandwidth data pipeline. The participating parts are called members of a trunk group. The Switch supports up to four trunk groups, the first three which may include from two to four Switch ports each and the fourth trunk which is the two GBIC ports (7x and 8x).

## Port Trunking


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Port Trunking
Monitor
User
Utilities
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232
DCE,9600,n,8,1
Power
Console
Speed
Link
Act
Full
Document: Done

Port Trunking Configuration

| Index | Description | Port Number | | | | | | | | Status | Active |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7-GBIC | 8-GBIC | | |
| 1 | | □ | □ | □ | □ | □ | □ | | | Disabled | Apply |
| 2 | | □ | □ | □ | □ | □ | □ | | | Disabled | Apply |
| 3 | | □ | □ | □ | □ | □ | □ | | | Disabled | Apply |
| 4 | | | | | | | | □ | □ | Disabled | Apply |

**Note**: A port can only belong to one trunk group.

**Figure 7-40. Port Trunking Configuration window**

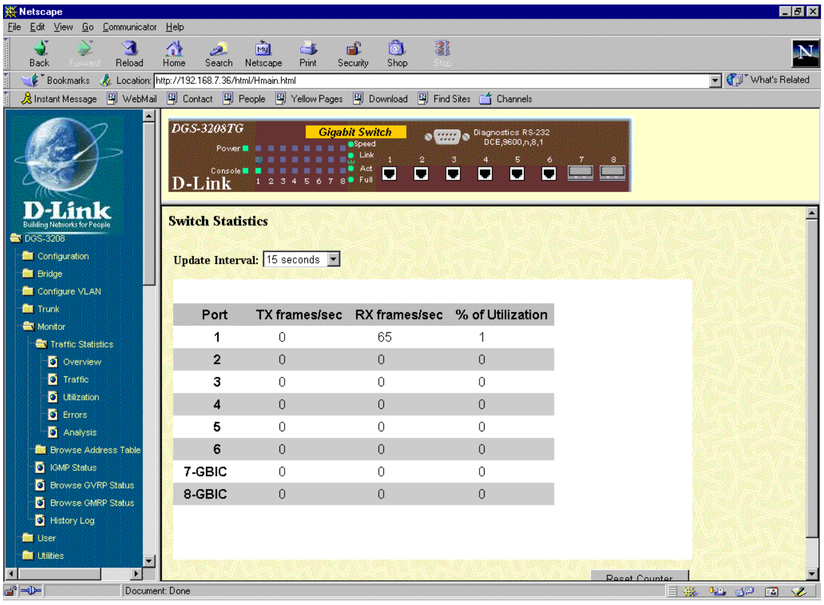
To create a trunk group, enter a description in the first textbox; then check the boxes for two or more ports (making sure none is used by any other trunk group), select the status you want (*Enabled* or *Disabled*), and click **Apply**. Please note that the maximum size for trunk groups 1 to 3 is four ports. Trunk group 4 is two ports.

# *Monitor*

This is the fifth category of the Web-based management program. The **Monitor** options include **Traffic Statistics** (**Overview**, **Traffic**, **Utilization**, **Errors**, and **Analysis**), **Browse Address Table** (**Search by MAC**, **Search By Port**, **Search By VLAN**, and **Search By None**), **IGMP Status**, **Browse GVRP Status**, **Browse GMRP Status**, and **History Log**. See below for explanations of each one.

## Traffic Statistics

### *Overview*



Switch Statistics

Update Interval: 15 seconds

| Port | TX frames/sec | RX frames/sec | % of Utilization |
|---|---|---|---|
| 1 | 0 | 65 | 1 |
| 2 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 |
| 7-GBIC | 0 | 0 | 0 |
| 8-GBIC | 0 | 0 | 0 |

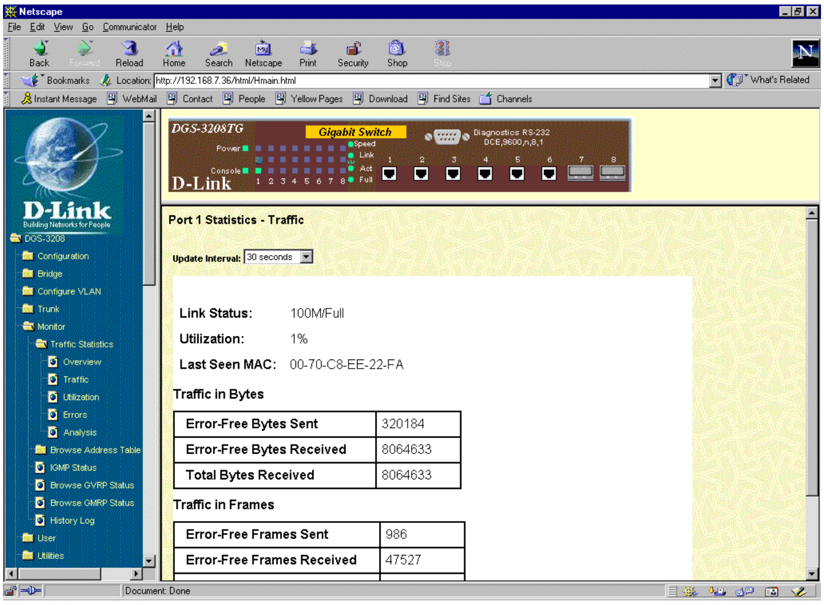
**Figure 7-41. Switch Statistics window**

Click **Reset Counter** to clear all the counters on the window above.

The information on this table is described as follows:

- **Update Interval** Choose the desired setting: *1 second*, *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.
- **TX frames/sec** Counts the total number of frames transmitted from a selected port per second since the Switch was last rebooted.
- **RX frames/sec** Counts all valid frames received on the port per second since the Switch was last rebooted.
- **% of Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval.

## *Traffic*



Port 1 Statistics - Traffic

Update Interval: 30 seconds

Link Status: 100M/Full

Utilization: 1%

Last Seen MAC: 00-70-C8-EE-22-FA

Traffic in Bytes

| | |
|---|---|
| Error-Free Bytes Sent | 320184 |
| Error-Free Bytes Received | 8064633 |
| Total Bytes Received | 8064633 |

Traffic in Frames

| | |
|---|---|
| Error-Free Frames Sent | 986 |
| Error-Free Frames Received | 47527 |

**Figure 7-42. Port Statistics – Traffic window**

The port statistics shown by default are those for the port you last configured. Once in the Traffic Statistics windows, you can click any port on the switch graphic to show statistics for that port. Click **Reset Counter** to clear all the counters on the window above.

The information is described as follows:

- **Update Interval** Choose the desired setting: *1 second*, *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.
- **Link Status** Indicates whether the port is online and working (*1000/Full/Flow control off* or *1000/Full/Flow control on*) or not (*Link Down*).
- **Utilization** Current utilization for the port, as a percentage of total available bandwidth.
- **Last Screen MAC** The last MAC address learned by the Switch.

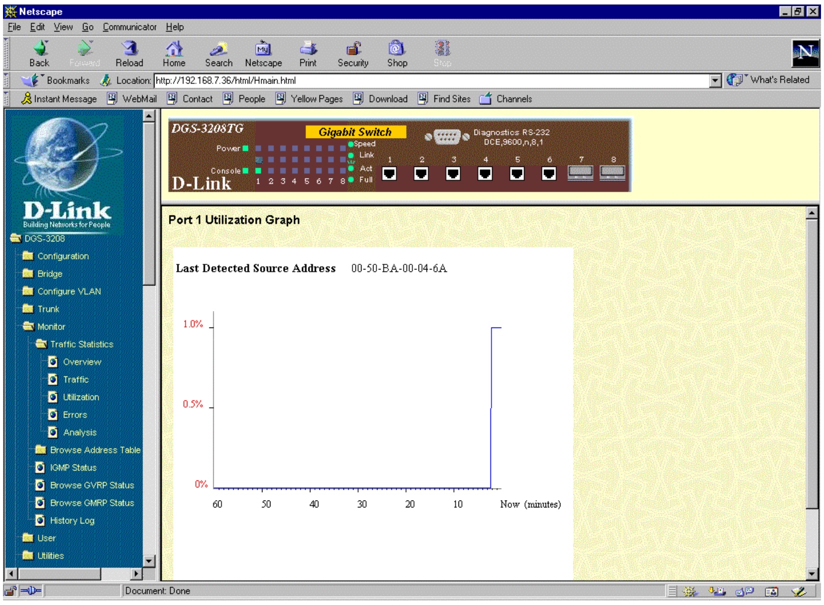
**Traffic in Bytes:**

- **Error-Free Bytes Sent** Counts the number of bytes successfully sent from the port.
- **Error-Free Bytes Received** Counts the total number of bytes (octets) included in valid (readable) frames.
- **Total Bytes Received** Counts the total number of bytes received on the port, whether in valid or invalid frames.

**Traffic in Frames:**

- **Error-Free Frames Sent** Counts the total number of frames transmitted from the port.
- **Error-Free Frames Received** Counts all valid frames received on the port.
- **Total Frames Received** Counts the number of frames received on the port, whether they were valid or not.

### *Utilization*


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
D-Link
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
Traffic Statistics
Overview
Traffic
Utilization
Errors
Analysis
Browse Address Table
IGMP Status
Browse GVRP Status
Browse GMRP Status
History Log
User
Utilities
1.0%
0.5%
0%
60
50
40
30
20
10
Now (minutes)
Document: Done

Port 1 Utilization Graph

Last Detected Source Address 00-50-BA-00-04-6A

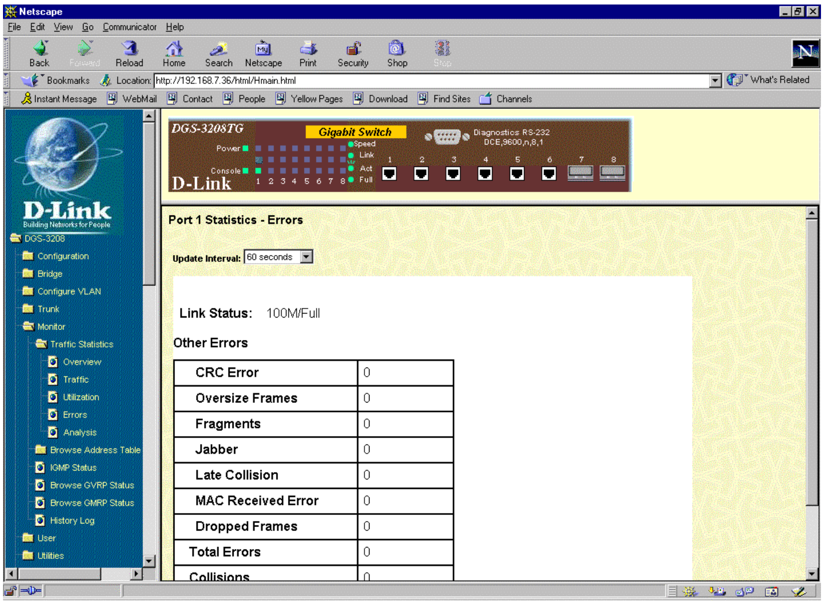
**Figure 7-43. Port Utilization Graph window**

Click **Reset Counter** to restart the graph on the window above.

The information is described as follows:

- **Last Detected Source Address** MAC address of the last source accessed.

### *Errors*


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
D-Link
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
Traffic Statistics
Overview
Traffic
Utilization
Errors
Analysis
Browse Address Table
IGMP Status
Browse GVRP Status
Browse GMRP Status
History Log
User
Utilities

Port 1 Statistics - Errors

Update Interval: 60 seconds

Link Status: 100M/Full

Other Errors

| | |
|---|---|
| CRC Error | 0 |
| Oversize Frames | 0 |
| Fragments | 0 |
| Jabber | 0 |
| Late Collision | 0 |
| MAC Received Error | 0 |
| Dropped Frames | 0 |
| Total Errors | 0 |
| Collisions | 0 |

**Figure 7-44. Port Statistics - Errors window**

Click **Reset Counter** to clear all the counters on the window above.

The information is described as follows:

- **Update Interval** Choose the desired setting: *1 second*, *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.

- **Link Status** Indicates whether the port is online and working (*1000/Full/Flow control off*, for example) or not (*Link Down*).

**Other Errors:**

- **CRC Error** Counts otherwise valid frames that did not end on a byte (octet) boundary.

- **Oversize Frames** Counts packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

- **Fragments** The number of good frames with length less than the 64-byte (octet) minimum defined by the Ethernet standard. These are usually caused by collisions.

- **Jabber** Counts frames longer than the maximum 1518 bytes (octets) with either bad framing or an invalid CRC.

- **Late Collision** Counts collisions that occur at or after the 64th byte (octet) in the frame. This may indicate that delays on your Ethernet are too long, and you have either exceeded the repeater count or cable length specified in the Ethernet standard.

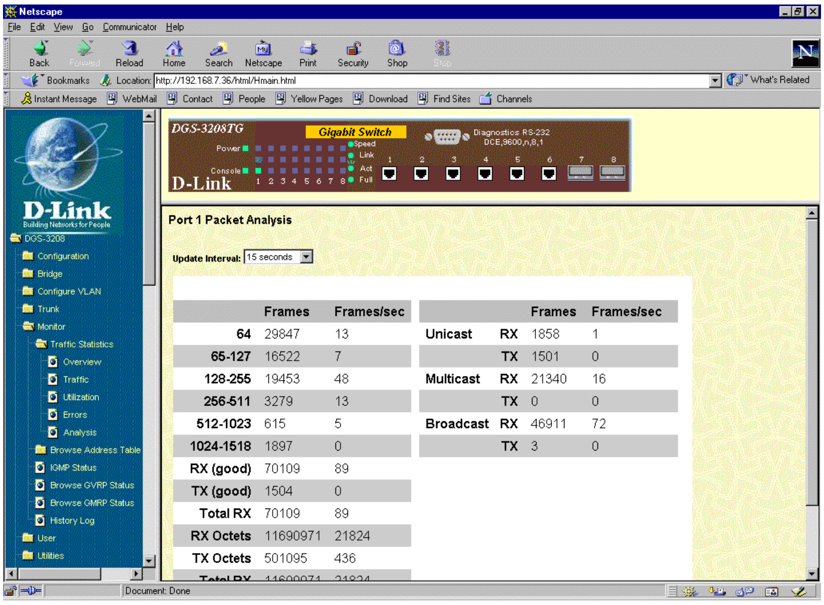
- **MAC Received Error** Counts bit patterns with illegal encodings. This may indicate noise on the line.

- **Dropped Frames** Counts received packets which are dropped due to any of the following reasons: lack of available receive buffers, port-disable, link-test-fail, spanning tree, or empty distribution list.

- **Total Errors** The sum of the CRC Error, Oversize Frames, Fragments, Jabber, Late Collision, MAC Received Error, and Dropped Frames counters.

- **Collisions** The best estimate of the total number of collisions on this Ethernet segment.

### *Analysis*



Port 1 Packet Analysis

Update Interval: 15 seconds

|  | Frames | Frames/sec |
|---|---|---|
| 64 | 29847 | 13 |
| 65-127 | 16522 | 7 |
| 128-255 | 19453 | 48 |
| 256-511 | 3279 | 13 |
| 512-1023 | 615 | 5 |
| 1024-1518 | 1897 | 0 |
| RX (good) | 70109 | 89 |
| TX (good) | 1504 | 0 |
| Total RX | 70109 | 89 |
| RX Octets | 11690971 | 21824 |
| TX Octets | 501095 | 436 |
| Total RX | 11690971 | 21824 |

|  |  | Frames | Frames/sec |
|---|---|---|---|
| Unicast | RX | 1858 | 1 |
|  | TX | 1501 | 0 |
| Multicast | RX | 21340 | 16 |
|  | TX | 0 | 0 |
| Broadcast | RX | 46911 | 72 |
|  | TX | 3 | 0 |

Figure 7-45. Port Packet Analysis window

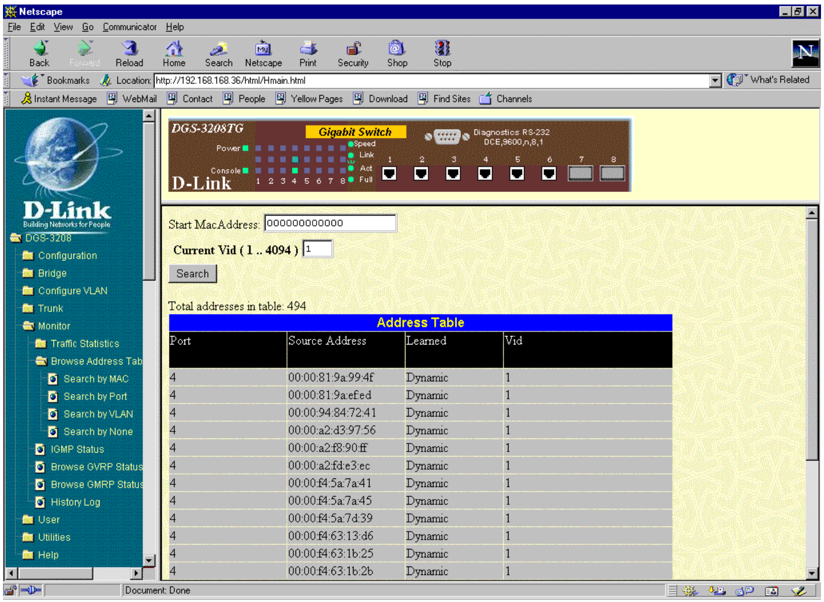
Click **Reset Counter** to clear all the counters on the window above.

The information is described as follows:

- **Update Interval** Choose the desired setting: *1 second*, *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.
- **64** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
- **65-127** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
- **128–255** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
- **256-511** The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
- **512-1023** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
- **1024-1518** 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).
- **RX (good)** The number of good frames received. This also includes local and dropped packets.
- **TX (good)** The number of good frames sent from the respective port.
- **Total RX** The number of frames received, good and bad.
- **Unicast Rx/Tx** The total number of good packets that were received by and directed to a unicast address. Note that this does not include dropped unicast packets
- **Multicast Rx/Tx** The total number of good packets that were received by and directed to a multicast address. Note that this number does not include packets directed to the broadcast address
- **Broadcast Rx/Tx** The total number of good packets that were received by and directed to a broadcast address. Note that this does not include multicast packets.

# Browse Address Table

## *Search By MAC*



Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.168.36/html/Hmain.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
Traffic Statistics
Browse Address Tab
Search by MAC
Search by Port
Search by VLAN
Search by None
IGMP Status
Browse GVRP Status
Browse GMRP Status
History Log
User
Utilities
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
Power Console Speed Link Act Full
D-Link
Document: Done

Start MacAddress: 000000000000

Current Vid ( 1 .. 4094 ) 1

Search

Total addresses in table: 494

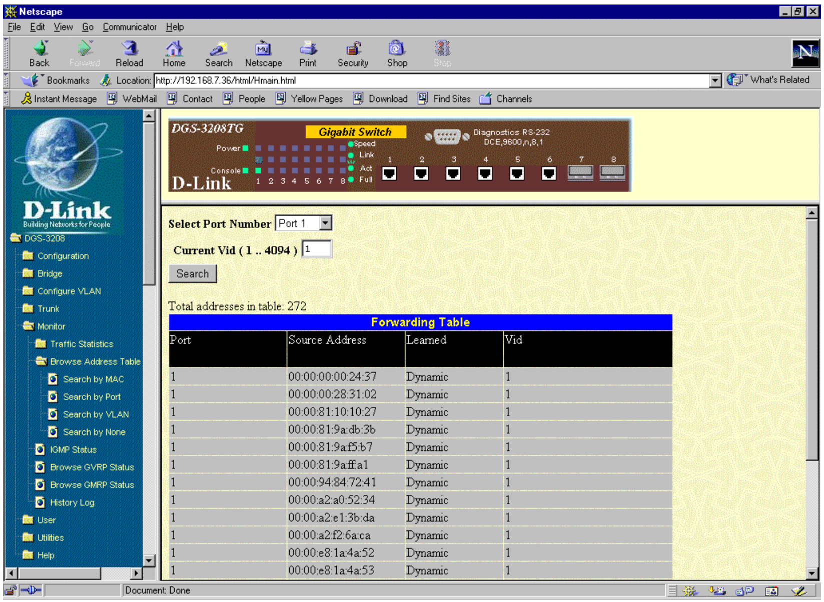
Address Table

| Port | Source Address | Learned | Vid |
|---|---|---|---|
| 4 | 00:00:81:9a:99:4f | Dynamic | 1 |
| 4 | 00:00:81:9a:ef:ed | Dynamic | 1 |
| 4 | 00:00:94:84:72:41 | Dynamic | 1 |
| 4 | 00:00:a2:d3:97:56 | Dynamic | 1 |
| 4 | 00:00:a2:f8:90:ff | Dynamic | 1 |
| 4 | 00:00:a2:fd:e3:ec | Dynamic | 1 |
| 4 | 00:00:f4:5a:7a:41 | Dynamic | 1 |
| 4 | 00:00:f4:5a:7a:45 | Dynamic | 1 |
| 4 | 00:00:f4:5a:7d:39 | Dynamic | 1 |
| 4 | 00:00:f4:63:13:d6 | Dynamic | 1 |
| 4 | 00:00:f4:63:1b:25 | Dynamic | 1 |
| 4 | 00:00:f4:63:1b:2b | Dynamic | 1 |

**Figure 7-46.  Address Table window**

The Switch allows you to display a forwarding table containing Switch ports, source addresses, learned statuses, and VLAN ID numbers. If the table doesn't display the information you want, fill in the requested information in the Start MAC Address and Current Vid (1..4094) fields and then click the **Search** button.

## *Search By Port*



Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
Traffic Statistics
Browse Address Table
Search by MAC
Search by Port
Search by VLAN
Search by None
IGMP Status
Browse GVRP Status
Browse GMRP Status
History Log
User
Utilities
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
Power Console Speed Link Act Full
D-Link
Document: Done

Select Port Number Port 1

Current Vid ( 1 .. 4094 ) 1

Search

Total addresses in table: 272

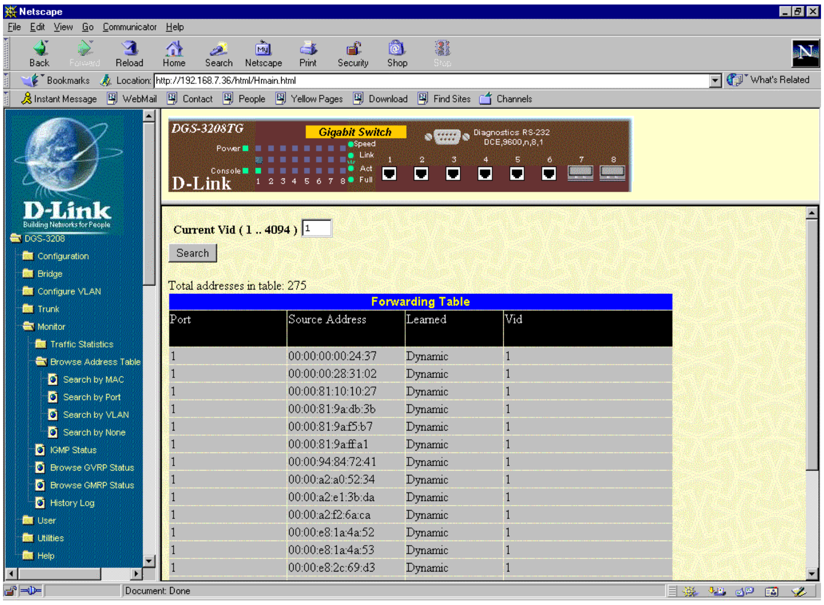
Forwarding Table

| Port | Source Address | Learned | Vid |
|---|---|---|---|
| 1 | 00:00:00:00:24:37 | Dynamic | 1 |
| 1 | 00:00:00:28:31:02 | Dynamic | 1 |
| 1 | 00:00:81:10:10:27 | Dynamic | 1 |
| 1 | 00:00:81:9a:db:3b | Dynamic | 1 |
| 1 | 00:00:81:9a:f5:b7 | Dynamic | 1 |
| 1 | 00:00:81:9a:ff:a1 | Dynamic | 1 |
| 1 | 00:00:94:84:72:41 | Dynamic | 1 |
| 1 | 00:00:a2:a0:52:34 | Dynamic | 1 |
| 1 | 00:00:a2:e1:3b:da | Dynamic | 1 |
| 1 | 00:00:a2:f2:6a:ca | Dynamic | 1 |
| 1 | 00:00:e8:1a:4a:52 | Dynamic | 1 |
| 1 | 00:00:e8:1a:4a:53 | Dynamic | 1 |

**Figure 7-47.  first Forwarding Table window**

The Switch allows you to display a forwarding table containing Switch ports, source addresses, learned statuses, and VLAN ID numbers. If the table doesn't display the information you want, fill in the requested information in the Select Port Number and Current Vid (1..4094) fields and then click the **Search** button.

### *Search By VLAN*



Current Vid ( 1 .. 4094 ) 1

Search

Total addresses in table: 275

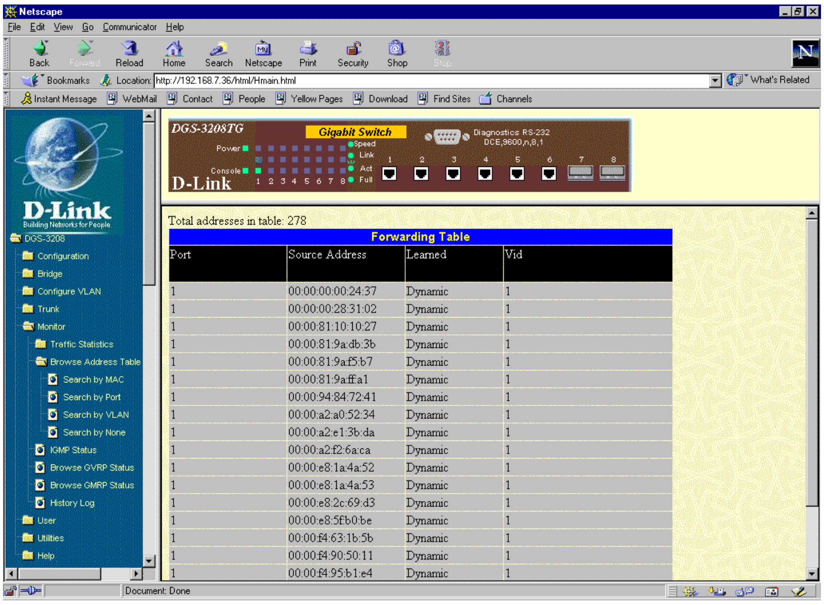
Forwarding Table

| Port | Source Address | Learned | Vid |
|---|---|---|---|
| 1 | 00:00:00:00:24:37 | Dynamic | 1 |
| 1 | 00:00:00:28:31:02 | Dynamic | 1 |
| 1 | 00:00:81:10:10:27 | Dynamic | 1 |
| 1 | 00:00:81:9a:db:3b | Dynamic | 1 |
| 1 | 00:00:81:9a:f5:b7 | Dynamic | 1 |
| 1 | 00:00:81:9a:ff:a1 | Dynamic | 1 |
| 1 | 00:00:94:84:72:41 | Dynamic | 1 |
| 1 | 00:00:a2:a0:52:34 | Dynamic | 1 |
| 1 | 00:00:a2:e1:3b:da | Dynamic | 1 |
| 1 | 00:00:a2:f2:6a:ca | Dynamic | 1 |
| 1 | 00:00:e8:1a:4a:52 | Dynamic | 1 |
| 1 | 00:00:e8:1a:4a:53 | Dynamic | 1 |
| 1 | 00:00:e8:2c:69:d3 | Dynamic | 1 |

**Figure 7-48. second Forwarding Table window**

The Switch allows you to display a forwarding table containing Switch ports, source addresses, learned statuses, and VLAN ID numbers. If the table doesn't display the information you want, fill in the requested information in the Current Vid (1..4094) field and then click the **Search** button.

### *Search By None*



Total addresses in table: 278

Forwarding Table

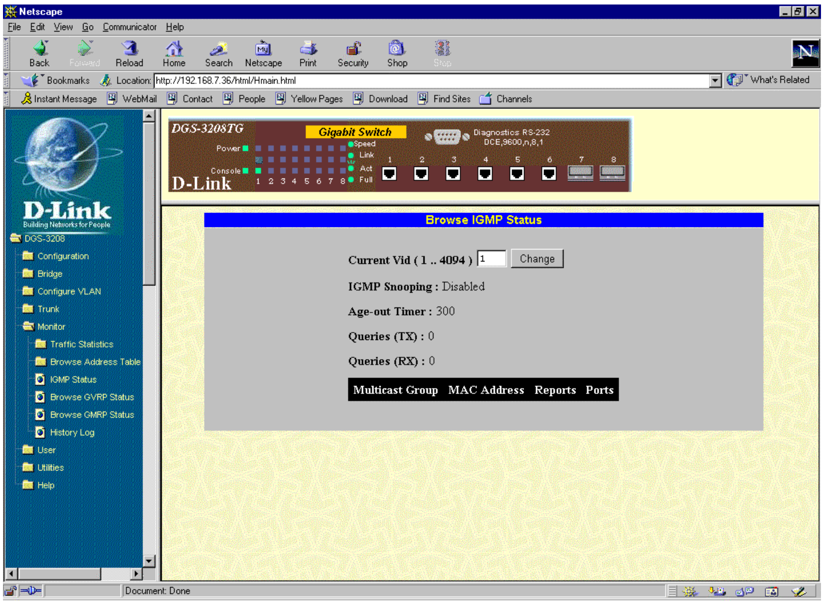
| Port | Source Address | Learned | Vid |
|---|---|---|---|
| 1 | 00:00:00:00:24:37 | Dynamic | 1 |
| 1 | 00:00:00:28:31:02 | Dynamic | 1 |
| 1 | 00:00:81:10:10:27 | Dynamic | 1 |
| 1 | 00:00:81:9a:db:3b | Dynamic | 1 |
| 1 | 00:00:81:9a:f5:b7 | Dynamic | 1 |
| 1 | 00:00:81:9a:ff:a1 | Dynamic | 1 |
| 1 | 00:00:94:84:72:41 | Dynamic | 1 |
| 1 | 00:00:a2:a0:52:34 | Dynamic | 1 |
| 1 | 00:00:a2:e1:3b:da | Dynamic | 1 |
| 1 | 00:00:a2:f2:6a:ca | Dynamic | 1 |
| 1 | 00:00:e8:1a:4a:52 | Dynamic | 1 |
| 1 | 00:00:e8:1a:4a:53 | Dynamic | 1 |
| 1 | 00:00:e8:2c:69:d3 | Dynamic | 1 |
| 1 | 00:00:e8:5f:b0:be | Dynamic | 1 |
| 1 | 00:00:f4:63:1b:5b | Dynamic | 1 |
| 1 | 00:00:f4:90:50:11 | Dynamic | 1 |
| 1 | 00:00:f4:95:b1:e4 | Dynamic | 1 |

**Figure 7-49. third Forwarding Table window**

The Switch allows you to display a forwarding table containing Switch ports, source addresses, learned statuses, and VLAN ID numbers.

## IGMP Status

The Monitor group's IGMP Status command lets you examine the operation of the Internet Group Management Protocol (IGMP). The Switch can recognize IGMP queries and reports sent between stations and an IGMP router. When enabled for IGMP snooping, the Switch can open or close a port to specific devices based on the IGMP messages sent from the device to the router or vice versa.



Browse IGMP Status

Current Vid ( 1 .. 4094 ) 1 Change

IGMP Snooping : Disabled

Age-out Timer : 300

Queries (TX) : 0

Queries (RX) : 0

| Multicast Group | MAC Address | Reports | Ports |
|---|---|---|---|

Figure 7-50. Browse IGMP Status window

This window displays the number of IGMP queries and reports for each active IP multicast group detected by the Switch. You can also view the current age-out timer as well as the IGMP snooping status. Enter the desired VLAN ID number in the Current Vid (1..4094) field and then click **Change**.

The fields displayed are defined as follows:

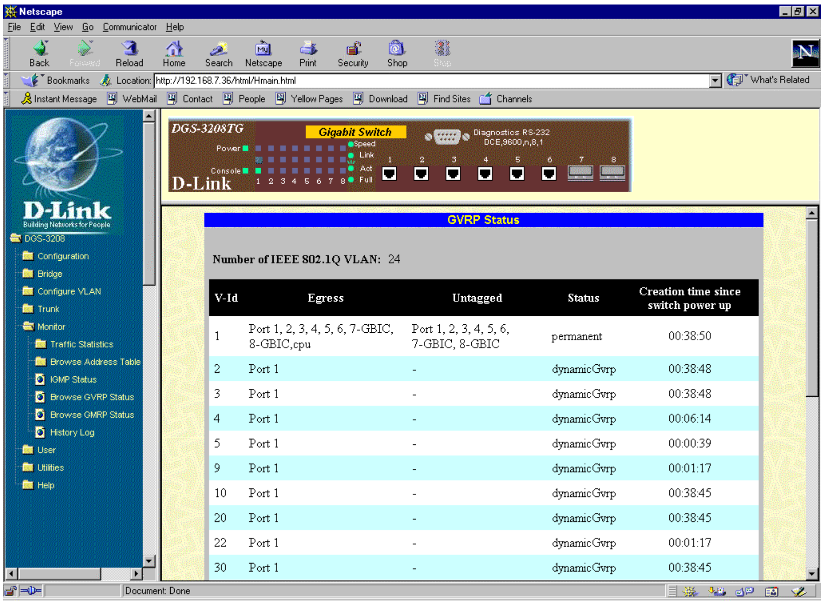
- **Current Vid (1..4094)** Enter the desired VLAN ID number in this field and then click the **Change** button.
- **IGMP Snooping** Indicates whether IGMP snooping is Enabled or Disabled.
- **Age-out Timer** Displays the time the Switch waits between IGMP queries.
- **Queries(TX)** The number of IGMP requests sent by the switch.
- **Queries(RX)** The number of IGMP requests that have arrived at a switch port.

A second table in the lower part of the window shows the following information:

- **Multicast Group** The Multicast IP address of the Multicast group being displayed.
- **MAC Address** The Multicast MAC address of the multicast group being displayed.
- **Reports** The number of notifications sent from each station to the IGMP host, signifying that the station is still (or wants to be) part of a multicast group.

- **Ports** The Switch ports supporting the selected multicast group.

## Browse GVRP Status



GVRP Status

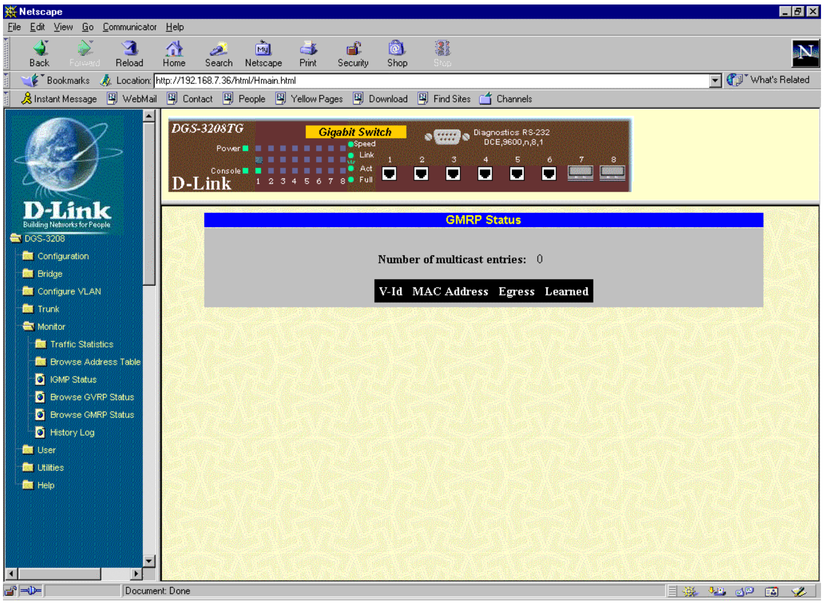
Number of IEEE 802.1Q VLAN: 24

| V-Id | Egress | Untagged | Status | Creation time since switch power up |
|---|---|---|---|---|
| 1 | Port 1, 2, 3, 4, 5, 6, 7-GBIC, 8-GBIC,cpu | Port 1, 2, 3, 4, 5, 6, 7-GBIC, 8-GBIC | permanent | 00:38:50 |
| 2 | Port 1 | - | dynamicGvrp | 00:38:48 |
| 3 | Port 1 | - | dynamicGvrp | 00:38:48 |
| 4 | Port 1 | - | dynamicGvrp | 00:06:14 |
| 5 | Port 1 | - | dynamicGvrp | 00:00:39 |
| 9 | Port 1 | - | dynamicGvrp | 00:01:17 |
| 10 | Port 1 | - | dynamicGvrp | 00:38:45 |
| 20 | Port 1 | - | dynamicGvrp | 00:38:45 |
| 22 | Port 1 | - | dynamicGvrp | 00:01:17 |
| 30 | Port 1 | - | dynamicGvrp | 00:38:45 |

**Figure 7-51. GVRP Status window**

This window contains information pertaining to GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP). Click the **Next** button at the bottom of the window to view the status of additional IEEE 802.1Q VLANs.

## Browse GMRP Status



GMRP Status

Number of multicast entries: 0

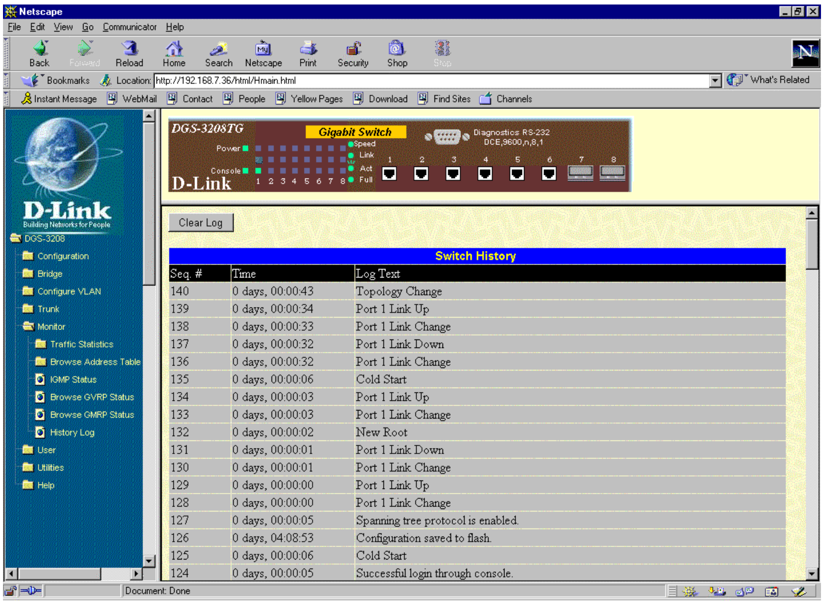
| V-Id | MAC Address | Egress | Learned |
|---|---|---|---|

**Figure 7-52. GMRP Status window**

This window contains information pertaining to the Group Multicast Registration Protocol (GMRP) status of IEEE 802.1Q VLANs.

## History Log

The Switch keeps a record of events that may be of interest to a network administrator: startups, reconfigurations, link activations and deactivations, firmware upgrades, and others.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
Traffic Statistics
Browse Address Table
IGMP Status
Browse GVRP Status
Browse GMRP Status
History Log
User
Utilities
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
Power
Console
Speed
Link
Act
Full
D-Link
Clear Log
Document: Done

Switch History

| Seq. # | Time | Log Text |
|---|---|---|
| 140 | 0 days, 00:00:43 | Topology Change |
| 139 | 0 days, 00:00:34 | Port 1 Link Up |
| 138 | 0 days, 00:00:33 | Port 1 Link Change |
| 137 | 0 days, 00:00:32 | Port 1 Link Down |
| 136 | 0 days, 00:00:32 | Port 1 Link Change |
| 135 | 0 days, 00:00:06 | Cold Start |
| 134 | 0 days, 00:00:03 | Port 1 Link Up |
| 133 | 0 days, 00:00:03 | Port 1 Link Change |
| 132 | 0 days, 00:00:02 | New Root |
| 131 | 0 days, 00:00:01 | Port 1 Link Down |
| 130 | 0 days, 00:00:01 | Port 1 Link Change |
| 129 | 0 days, 00:00:00 | Port 1 Link Up |
| 128 | 0 days, 00:00:00 | Port 1 Link Change |
| 127 | 0 days, 00:00:05 | Spanning tree protocol is enabled. |
| 126 | 0 days, 04:08:53 | Configuration saved to flash. |
| 125 | 0 days, 00:00:06 | Cold Start |
| 124 | 0 days, 00:00:05 | Successful login through console. |

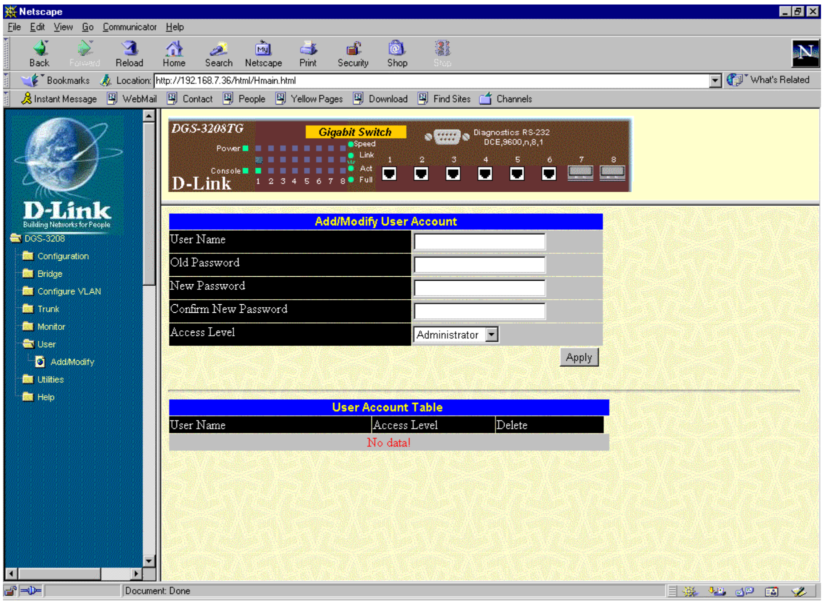
**Figure 7-53. Switch History window**

The Switch can be commanded to upload its history via TFTP to a machine you specify. See the description of the Utilities group’s Upload History command, further on in this chapter.

# *User*

This is the sixth category of the Web-based management program. One item is featured in this section, **Add/Modify User Account**.

## Add/Modify


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
D-Link
D-Link Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Add/Modify
Utilities
Help
Document: Done

**Add/Modify User Account**

| | |
|---|---|
| User Name | |
| Old Password | |
| New Password | |
| Confirm New Password | |
| Access Level | Administrator |

Apply

**User Account Table**

| User Name | Access Level | Delete |
|---|---|---|
| No data! | | |

**Figure 7-54. Add/Modify User Account window**

To add or change a User Account, fill in the appropriate information in the User Name, Old Password, New Password, and Confirm New Password fields. Then select *Normal User* or *Administrator* in the Access Level control and click **Apply**.

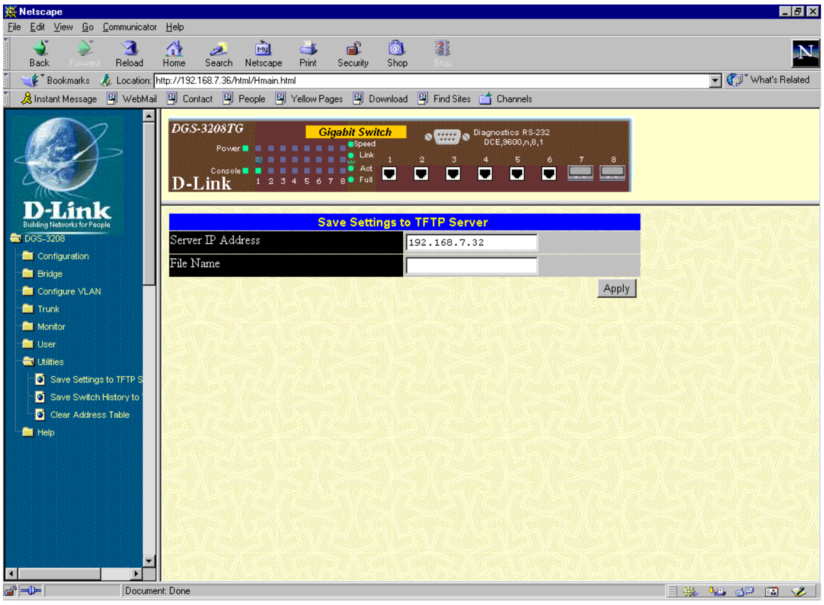
To delete a User Account, click the "X" icon in the delete column on the User Account Table at the bottom of the window.

# *Utilities*

This is the seventh category of the Web-based management program. The **Utilities** options include **Save Settings to TFTP Server**, **Save Switch History to TFTP Server**, and **Clear Address Table**. See below for explanations of each one.

## Save Settings to TFTP Server

This function lets you retrieve the Switch's current configuration and save it for later use in configuring this or an identical switch.



Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Save Settings to TFTP S
Save Switch History to
Clear Address Table
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232
DCE,9600,n,8,1
Document: Done

Save Settings to TFTP Server

| | |
|---|---|
| Server IP Address | 192.168.7.32 |
| File Name | |

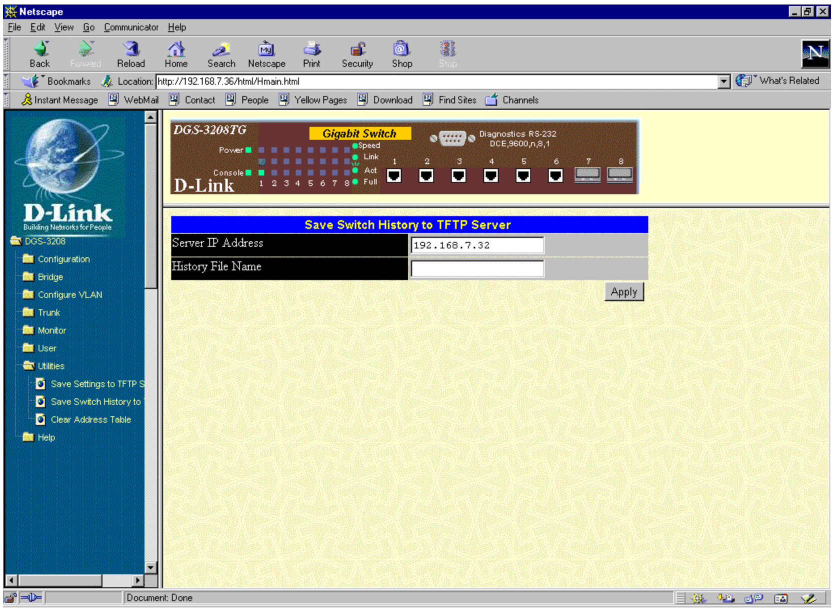
Apply

Figure 7-55. Save Settings to TFTP Server window

To have an image of the Switch's current configuration uploaded to a TFTP server on your network, enter the server's IP address, supply a valid file name, and click **Apply**.

## Save Switch History to TFTP Server

The Switch keeps a record of events that may be of interest to a network administrator: startups, reconfigurations, link activations and deactivations, firmware upgrades, and others. You can view this record by choosing **History Log** from the **Monitor** command group.



Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Save Settings to TFTP S
Save Switch History to
Clear Address Table
Help
DGS-3208TG
Gigabit Switch
Diagnostics RS-232
DCE,9600,n,8,1
Document: Done

Save Switch History to TFTP Server

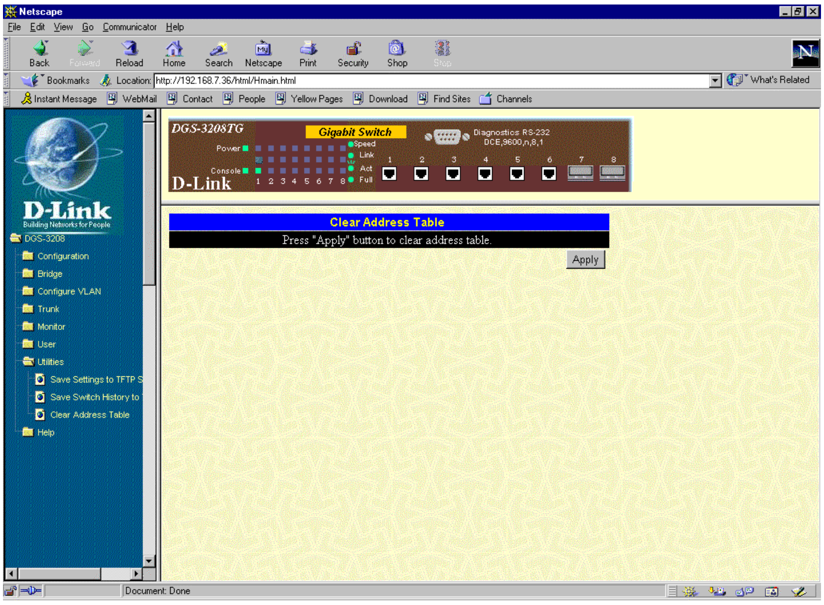
| | |
|---|---|
| Server IP Address | 192.168.7.32 |
| History File Name | |

Apply

Figure 7-56. Save Switch History to TFTP Server window

To have a record of recent operational events uploaded to a TFTP server on your network, enter the server's IP address, supply a valid file name, and click **Apply**.

## Clear Address Table


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
D-Link
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Save Settings to TFTP S
Save Switch History to
Clear Address Table
Help
Document: Done

Clear Address Table

Press "Apply" button to clear address table.

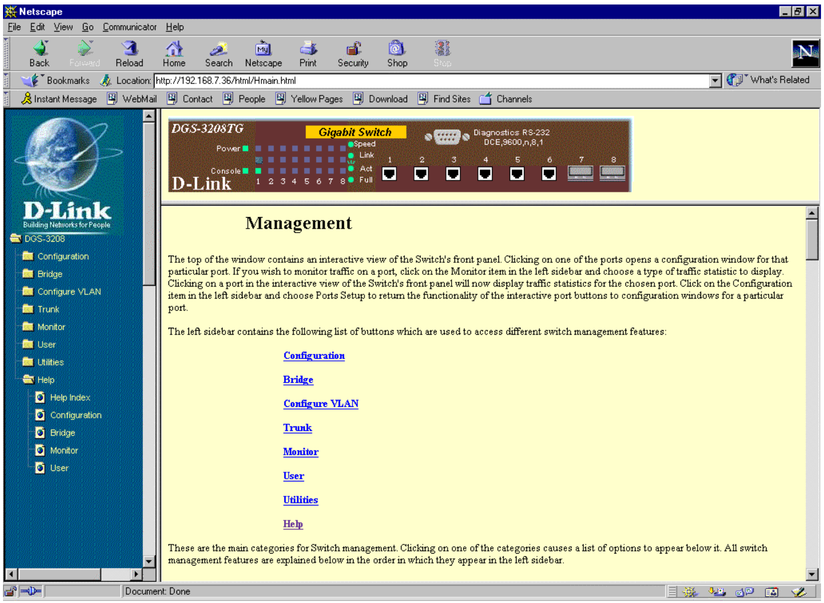
Apply

Figure 7-57. Clear Address Tables window

Click **Apply** to clear all address tables.

# *Help*

Click this button to access the online help files for the Switch.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.7.36/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
DGS-3208TG
Gigabit Switch
Diagnostics RS-232 DCE,9600,n,8,1
D-Link
DGS-3208
Configuration
Bridge
Configure VLAN
Trunk
Monitor
User
Utilities
Help
Help Index
Configuration
Bridge
Monitor
User
Document: Done

Management

The top of the window contains an interactive view of the Switch's front panel. Clicking on one of the ports opens a configuration window for that particular port. If you wish to monitor traffic on a port, click on the Monitor item in the left sidebar and choose a type of traffic statistic to display. Clicking on a port in the interactive view of the Switch's front panel will now display traffic statistics for the chosen port. Click on the Configuration item in the left sidebar and choose Ports Setup to return the functionality of the interactive port buttons to configuration windows for a particular port.

The left sidebar contains the following list of buttons which are used to access different switch management features:

Configuration

Bridge

Configure VLAN

Trunk

Monitor

User

Utilities

Help

These are the main categories for Switch management. Clicking on one of the categories causes a list of options to appear below it. All switch management features are explained below in the order in which they appear in the left sidebar.

Figure 7-58. Help window

# A

# TECHNICAL SPECIFICATIONS

| General | |
|---|---|
| Standards: | IEEE 802.3u, 802.3ab, 802.3x, 802.3z, and GBIC<br>IEEE 802.3 Frame types: Transparent<br>IEEE 802.3 MAC layer frame size: 64–1518 bytes |
| Protocol: | CSMA/CD |
| Data Transfer Rate: | Gigabit Ethernet: 2000 Mbps (full duplex) |
| Topology: | Star |
| Network Cables: | 1000BASE-T ports: four-pair Category 5 UTP (max. 100 m).<br>Optical fiber GBICs: 50/125-micron multimode fiber (max. 525 m), 62.5/125-micron multimode fiber (max. 275 m) |
| Number of Ports: | Eight (six 1000BASE-T 100/1000-Mbps ports and two GBIC slots) |

| Physical and Environmental | |
|---|---|
| AC inputs: | 100 ~ 240 VAC, 50 ~ 60 Hz (internal universal power supply) |
| Power Consumption: | 75 watts maximum |
| DC fans: | Three built-in 40 x 40 mm DC fans |
| Operating Temperature: | 0 to 50 degrees Celsius |
| Storage Temperature: | -25 to 55 degrees Celsius |
| Humidity: | 5% to 95% RH, non-condensing |
| Dimensions: | 441 mm x 367 mm x 44 mm (1U), 19-inch rack-mount width |
| Weight: | 5 kg |
| EMI: | FCC Class A, CE Mark Class A, VCCI Class A, BSMI Class A, C-Tick Class A |
| Safety: | UL (UL 1950), CSA (CSA950), TÜV/GS (EN60950) |

| Performance | |
|---|---|
| Transmission Method: | Store-and-forward |
| RAM Buffer: | 16 Mbytes per device *83.3 MHz |
| Filtering Address Table: | 12K MAC addresses per device |
| Packet Filtering/Forwarding Rate: | 1,488,100 pps per port |
| MAC Address Learning: | Auto-learning and auto-aging |

# INDEX

# D-Link® Offices

AUSTRALIA
**D-LINK AUSTRALASIA**
Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077
TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand)
URL: www.dlink.com.au E-MAIL: support@dlink.com.au, info@dlink.com.au

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

CHILE
**D-LINK SOUTH AMERICA**
Isidora Goyenechea #2934 of.702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-2320923 URL: www.dlink.cl
E-MAIL: ccasassu@dlink.cl, tsilva@dlink.cl

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

EGYPT
**D-LINK MIDDLE EAST**
7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-2456176 FAX: 202-2456192 URL: www.dlink-me.com
E-MAIL: support@dlink-me.com, fateen@dlink-me.com

FRANCE
**D-LINK FRANCE**
Le Florilege #2, Allee de la Fresnerie 78330 Fontenay Le Fleury France
TEL: 33-1-30238688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr E-MAIL: info@dlink-france.fr

GERMANY
**D-LINK GERMANY**
Bachstrae 22, D-65830 Kriftel Germany
TEL: 49-(0)6192-97110 FAX: 49-(0)6192-9711-11 URL: www.dlink.de
BBS: 49-(0)6192-971199 (Analog) 49-(0)6192-971198 (ISDN)
INFO LINE: 00800-7250-0000 (toll free) HELP LINE: 00800-7250-4000 (toll free)
REPAIR LINE: 00800-7250-8000 E-MAIL: mbischoff@dlink.de, mboerner@dlink.de

INDIA
**D-LINK INDIA**
Plot No.5, Kurla-Bandra Complex Road, Off Cst Road, Santacruz (E), Bombay - 400 098 India
TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: www.dlink-india.com E-MAIL: service@dlink.india.com

ITALY
**D-LINK ITALY**
Via Nino Bonnet No. 6/b, 20154 Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 E-MAIL: info@dlink.it URL: www.dlink.it

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

RUSSIA
**D-LINK RUSSIA**
Michurinski Prospekt 49, 117607 Moscow, Russia
TEL: 7-095-737-3389, 7-095-737-3492 FAX: 7-095-737-3390 E-MAIL: vl@dlink.ru

SINGAPORE
**D-LINK INTERNATIONAL**
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL: 65-774-6233 FAX: 65-774-6322 URL: www.dlink-intl.com E-MAIL: info@dlink.com.sg

S. AFRICA
**D-LINK SOUTH AFRICA**
Unit 2, Parkside 86 Oak Avenue
Highveld Technopark Centurion, Gauteng, Republic of South Africa
TEL: 27(0)126652165 FAX: 27(0)126652186 CELL NO: 0826010806 (Bertus Moller)
CELL NO: 0826060013 (Attie Pienaar) E-MAIL: bertus@d-link.co.za, attie@d-link.co.za

SWEDEN
**D-LINK SWEDEN**
P.O. Box 15036, S-167 15 Bromma Sweden
TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901 E-MAIL: info@dlink.se URL: www.dlink.se

TAIWAN
**D-LINK TAIWAN**
2F, No. 119 Pao-Chung Road, Hsin-Tien, Taipei, Taiwan, R.O.C.
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 URL: www.dlinktw.com.tw E-MAIL: dssqa@tsc.dlinktw.com.tw

U.K.
**D-LINK EUROPE**
D-Link House, 6 Garland Road, Stanmore, London HA7 1DP U.K.
TEL: 44-20-8235-5555 FAX: 44-20-8235-5500 BBS: 44-20-8235-5511 URL: www.dlink.co.uk
E-MAIL: info@dlink.co.uk

**U.S.A**

**D-LINK U.S.A.**
53 Discovery Drive, Irvine, CA 92618 USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033 INFO LINE: 1-800-326-1688 BBS: 1-949-455-1779, 1-949-455-9616
URL: www.dlink.com E-MAIL: tech@dlink.com, support@dlink.com

# Registration Card

***Print, type or use block letters.***

Your name: Mr./Ms______________________________________________________________________
Organization: ________________________________________Dept. _________________________
Your title at organization:____________________________________________________________
Telephone:________________________________ Fax:________________________________
Organization's full address: ___________________________________________________________
_______________________________________________________________________________
Country: _______________________________________________________________________
Date of purchase (Month/Day/Year): _____________________________________________________

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

(* Applies to adapters only)

## *Product was purchased from:*

Reseller's name: ________________________________________________________________
Telephone:________________________________ Fax:________________________________
Reseller's full address: _________________________________________________________
_____________________________________________________________
_____________________________________________________________

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

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

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

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

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

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

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

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

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

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

***10.Your comments on this product?***
_______________________________________________________________________________

PLEASE
PLACE STAMP
HERE

TO:

D-Link®