

DGS-3224TG

Managed 24-Port Gigabit Ethernet Switch

User's Guide

First Edition (May 2002)

651TG3224015

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. Verwenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehöerteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät ist 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 sollte 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 autorisiertem 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 sind beschädigt.
 - b – Flüssigkeit ist in das Gerät eingedrungen.
 - c – Das Gerät war Feuchtigkeit ausgesetzt.
 - d – Wenn das Gerät nicht der Bedienungsanleitung entsprechend 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 Originalersatzteile bzw. den Originalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Reparatur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm² einzusetzen.

Trademarks

Copyright D-Link Corporation ©2002. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

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

Limited Warranty

Hardware:

D-Link warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following periods measured from date of purchase from D-Link or its Authorized Reseller:

<u>Product Type</u>	<u>Warranty Period</u>
Complete products	One year
Spare parts and spare kits	90 days

The one-year period of warranty on complete products applies on condition that the product's 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. Failing such timely registration of purchase, the warranty period shall be limited to 90 days.

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 will ordinarily reimburse Purchaser for mailing/shipping/insurance expenses incurred for return of defective product in accordance with this warranty. 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 licence 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.

LIMITATION OF WARRANTIES

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, NEGLIGENCE, 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.

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 addresses/telephone/fax list of D-Link offices is provided in the back of this manual.

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 Funkstörungen 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 caso, 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.

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	1
Overview of this User's Guide	1
Introduction	2
Features	2
Ports	2
Performance Features	2
Management	3
Unpacking and Setup.....	4
Unpacking.....	4
Installation	4
Desktop or Shelf Installation	4
Rack Installation.....	5
Power on.....	6
Power Failure	6
Identifying External Components	7
Front Panel.....	7
Rear Panel.....	7
Side Panels.....	8
LED Indicators	8
Connecting The Switch.....	9
Switch to End Node	9
Switch to Hub or Switch	9
Switch Management and Operating Concepts	11
Local Console Management	11
Diagnostic (console) port (RS-232 DCE).....	11
IP Addresses and SNMP Community Names	12
Traps.....	13
MIBs.....	14
SNMP	14
Authentication	15
Packet Forwarding.....	15
MAC Address Aging Time	15
Filtering.....	15
Spanning Tree Protocol.....	16
STP Operation Levels	16
Bridge Protocol Data Units	17
Creating a Stable STP Topology	18
STP Port States	18
User-Changeable STP Parameters	20
Illustration of STP	20
VLANs	22
Notes About VLANs on the DGS-3224TG.....	22
IEEE 802.1Q VLANs.....	22
802.1Q VLAN Packet Forwarding	23
802.1Q VLAN Tags	24
Port VLAN ID.....	25
Tagging and Untagging.....	26

Ingress Filtering	26
DHCP	27
Configuring the Switch Using the Console Interface	29
Before You Start	29
Connecting to the Switch	29
User Accounts Management	32
Save Changes	34
Factory Reset	35
Configuration	38
Configure IP Address	39
Configure Switch Information and Advanced Settings	41
Configure Ports	43
Configure Spanning Tree Protocol	44
Configure Static (Destination-Address Forwarding) Table	46
Configure VLANs	49
Configure IGMP Snooping	53
Configure Trunk	55
Configure Port Mirroring	56
Configure Class of Service, Default Priority, and Traffic Class	57
Configure RS232 and SLIP	60
Network Monitoring	61
Port Utilization	62
Port Error Packets	63
Port Packet Analysis	63
Browse MAC Address	64
Switch History	65
IGMP Snooping	66
Browse Multicast Status	67
VLAN Status	68
SNMP Manager Configuration	68
System Utilities	69
Upgrade Firmware from TFTP Server	70
Use Configuration File on TFTP Server	71
Save Settings to TFTP Server	72
Save History Log to TFTP Server	73
Ping Test	74
Reboot	75
Web-Based Network Management	78
Introduction	78
Getting Started	78
Configuration	82
IP Address	82
Switch Information	83
Advanced Settings	84
Port Configuration	85
Port Mirroring	86
Port Trunking	87
IGMP Snooping	87
Spanning Tree	88
Static Forwarding Table	91
VLANs	92
Port Default Priority	95
Class of Traffic	96
Class of Service	96
RS232 & SLIP	98

Management.....	99
Security IP	99
SNMP Manager	99
Trap Manager.....	100
User Accounts.....	100
Monitoring.....	101
Port Utilization	101
Packets	102
Errors	108
Size	113
MAC Address Table	115
IGMP Snooping Table	116
VLAN Multicast Table.....	117
IGMP Multicast Table	117
VLAN Status	117
Maintenance.....	118
TFTP Services.....	118
Switch History.....	120
Ping Test	121
Save Changes.....	122
Factory Reset	123
Restart System.....	123
Connection Timeout	124
Logout.....	124
Help.....	124
Technical Specifications	125
Cable Lengths	128
Runtime Switching Software Default Settings.....	129
Understanding and Troubleshooting the Spanning Tree Protocol.....	130
Blocking State	130
Listening State	131
Learning State.....	132
Forwarding State.....	133
Disabled State.....	134
Troubleshooting STP.....	135
Spanning Tree Protocol Failure	135
Full/Half Duplex Mismatch.....	136
Unidirectional Link	137
Packet Corruption.....	138
Resource Errors	138
Identifying a Data Loop	138
Avoiding Trouble	138
Brief Review of Bitwise Logical Operations.....	141
Index.....	142

ABOUT THIS GUIDE

This User's guide tells you how to install your DGS-3224TG, how to connect it to your Gigabit Ethernet network, and how to set its configuration using the built-in console interface.

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, and LED indicators of the Switch.
- Chapter 4, "*Connecting the Switch.*" Tells how you can connect the DGS-3224TG to your Gigabit Ethernet network.
- Chapter 5, "*Switch Management and Operating 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-3224TG.
- Appendix B, "*Cable Lengths.*" Contains chart for fiber-optic and copper cable maximum distances.
- Appendix C, "*Factory Default Settings.*"
- Appendix D, "*Understanding and Troubleshooting the Spanning Tree Protocol.*"
- Appendix E, "*Brief Review of Bitwise Logical Operations.*"

1

INTRODUCTION

This section describes the features of the DGS-3224TG.

Features

The DGS-3224TG was designed for departmental and enterprise connections. As an all-gigabit-port switch, it is ideal for backbone and server connection. Powerful and versatile, the switch eliminates network bottlenecks while giving users the capability to fine-tune performance

Switch features include:

Ports

- Twenty high performance 1000BASE-T ports for making 10/100/1000 connections to a backbone, end stations, and servers.
- Four GBIC ports to connect fiber optic media to another switch, server or network backbone.
- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

Performance Features

- Store-and-forward switching scheme.
- High-speed data forwarding rate of 1,488,100 pps per port at 100% of wire-speed for 1000 Mbps speed.
- Optimized 32K entry address database without flooding.
- 802.1D Spanning Tree support. Can be disabled on the entire switch or on a per-port basis.
- 802.1Q Tagged VLAN support, including GVRP (GARP VLAN Registration Protocol).
- Support for 200 VLANs in total, including 64 static VLANs.
- IGMP snooping support per switch.
- Link aggregation support for up to 6 trunk groups and 16 trunk members per group.

Management

- RS-232 console port for out-of-band network management via a console terminal.
- Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops.
- SNMP V.1.
- Fully configurable either in-band or out-of-band control via SNMP based software.
- Flash memory for software upgrades. This can be done in-band via TFTP or out-of-band via the console.
- Built-in SNMP management:
 - Bridge MIB (RFC 1493)
 - MIB-II (RFC 1213)
 - 802.1P/Q MIB (RFC 2674)
 - Interface MIB (RFC 2233)
 - Mini-RMON MIB (RFC 1757) – 4 groups. The RMON specification defines the counters for the receive functions only. However, the DGS-3224TG provides counters for both receive and transmit functions.
- Supports Web-based management.
- TFTP support.
- BOOTP support.
- DHCP Client support.
- Password enabled.
- Telnet remote control console.

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-3224TG 24-Port Gigabit Ethernet Switch
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This User's Guide with Registration Card

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

Installation

Use the following guidelines when choosing a place to install the switch:

- The surface must support at least 6.5 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 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 should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow adequate space for ventilation between the device and the objects around it.

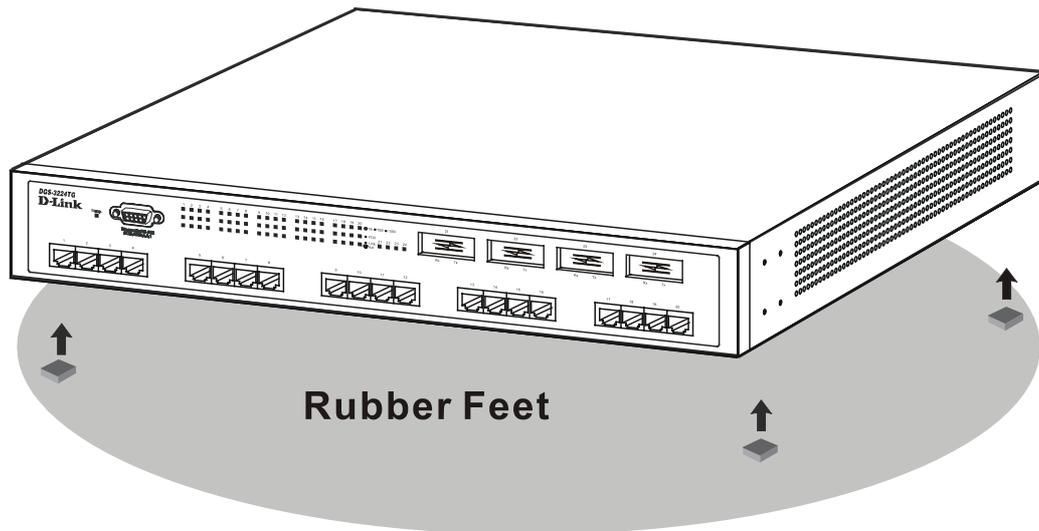


Figure 2-1. Installing rubber feet for desktop installation

Rack Installation

The DGS-3224TG can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.

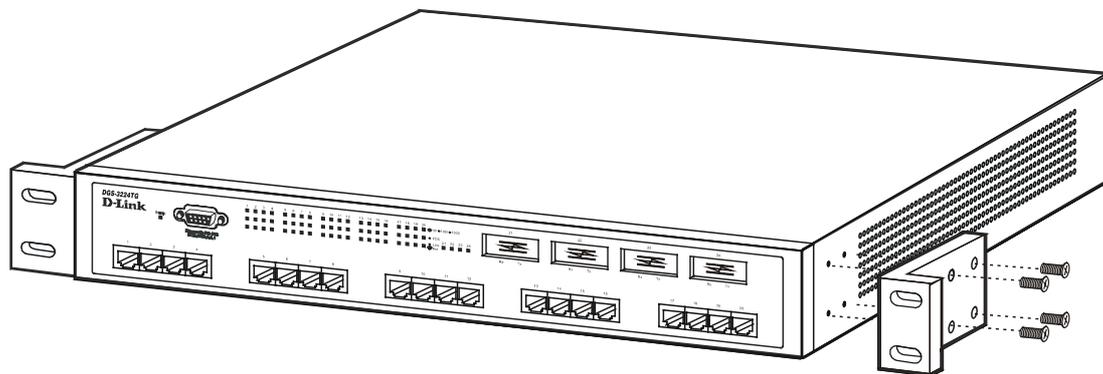


Figure 2- 2A. Attaching the mounting brackets

Then, use the screws provided with the equipment rack to mount the witch on the rack.

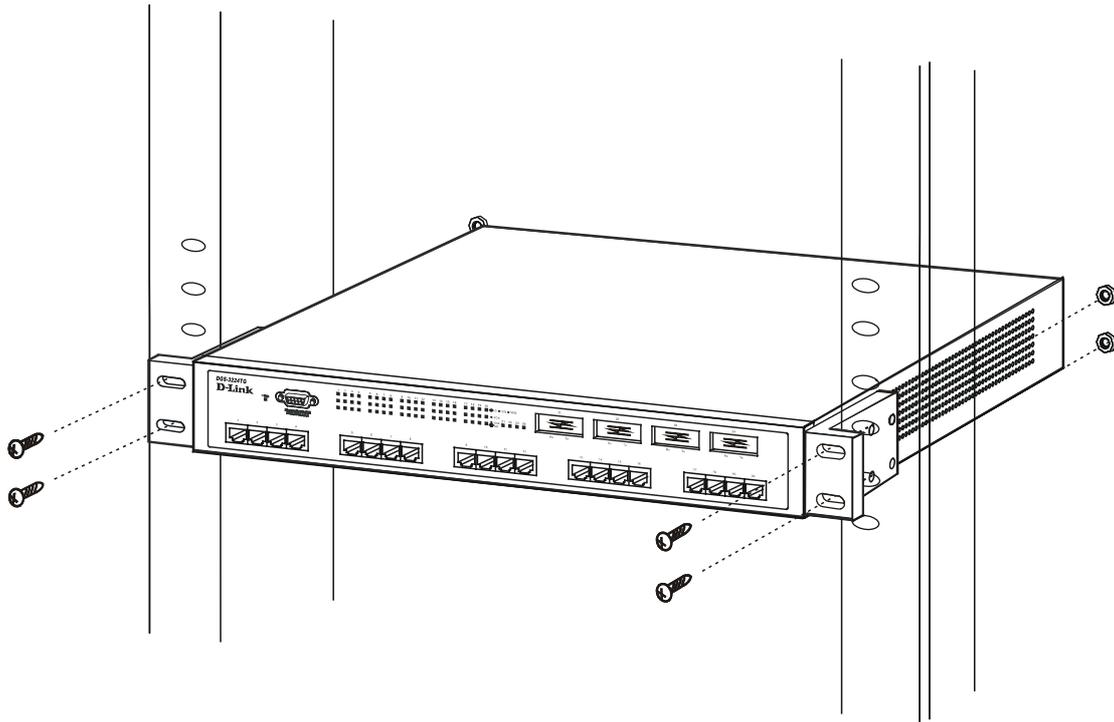


Figure 2-2B. Installing in an equipment rack

Power on

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

After the switch is plugged in, the LED indicators should respond as follows:

- All LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.
- The power LED indicator will blink while the switch loads onboard software and performs a self-test. After approximately 20 seconds, the LED will light again to indicate the switch is in a ready state.

Power Failure

As a precaution in the event of a power failure, unplug the switch. 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 DGS-3224TG.

Front Panel

The front panel of the switch consists of LED indicators, an RS-232 communication port, 20 1000BASE-T ports, and 4 GBIC ports.

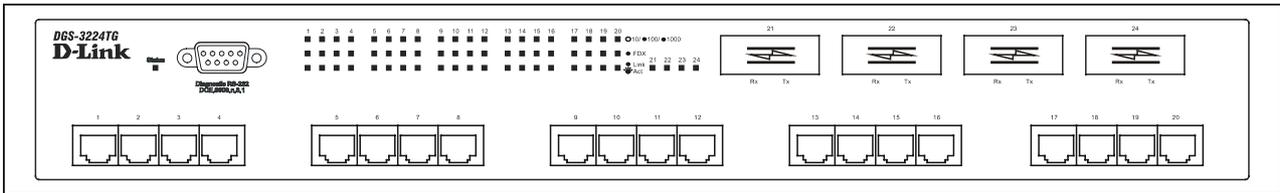


Figure 3-1. Front panel view

- An RS-232 DCE console port for setting up and managing the switch via a connection to a console terminal or PC using a terminal emulation program.
- Comprehensive LED indicators display the status of the switch and the network (see the *LED Indicators* section below).
- Four GBIC ports to connect fiber optic media to another switch, server, or network backbone.
- Twenty 1000BASE-T Ethernet ports for 10/100/1000 connections to a backbone, end stations, and servers.

Rear Panel

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



Figure 3-2. Rear panel view

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

Side Panels

The right side panel of the switch contains two system fans (see the top part of the diagram below). The left side panel contains heat vents.

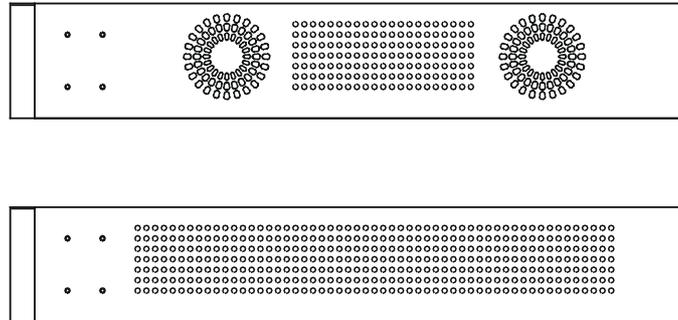


Figure 3-3. Side panel views of the Switch

- The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

LED Indicators

The LED indicators of the switch include Status, Speed, Full Duplex, and Link/Activity. The following shows the LED indicators for the switch along with an explanation of each indicator.

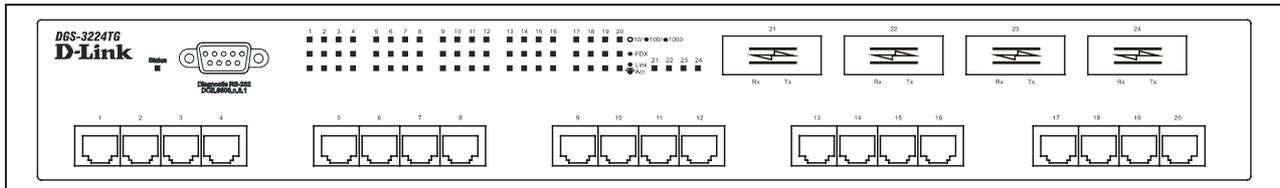


Figure 3-4. LED indicators

- **Status** – This indicator on the front panel blinks green when the system is booting up. It is solid green when the system is operating normally and solid red if the system fails.
- **Speed** – There are three rows of indicators for the 20 copper ports. The top LED is solid green for 1000 Mbps connections and solid amber for 100 Mbps connections. The indicator is off for 10 Mbps connections.
- **Full Duplex** – This indicator for the 20 copper ports is located in the middle row. Solid green indicates a full-duplex connection. The LED is off for half-duplex connections.
- **Act/Link** – This indicator is located in the bottom row for the 20 copper ports and directly to the left of the four GBIC ports. In each case, these indicators light solid green when there is a secure connection (or link) to a device on any of the ports. The LEDs blink green whenever there is reception or transmission (i.e. Activity--Act) of data occurring on a port.

4

CONNECTING THE SWITCH

This chapter describes how to connect the DGS-3224TG to your Gigabit Ethernet network.

Switch to End Node

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

An end node can be connected to the switch via a two-pair Category 3, 4, 5, or 5e UTP/STP cable—for optimal performance, Category 5e is recommended. The end node should be connected to any of the ports of the switch.

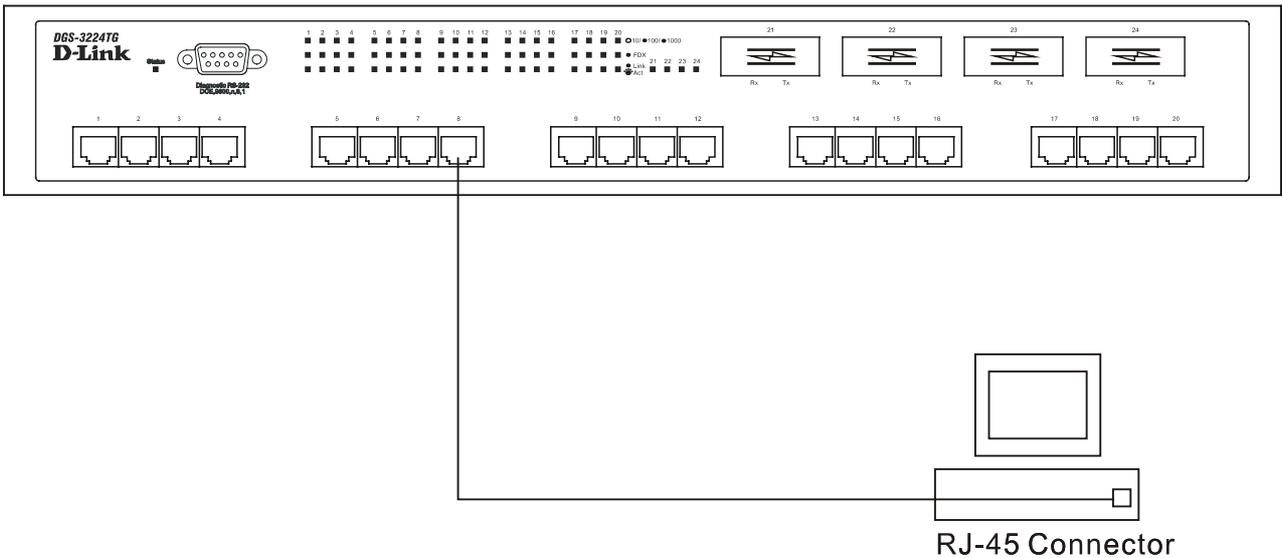


Figure 4-1. Switch connected to an End Node

The **Link/Act** LEDs on the bottom row of the front panel of the device light green when the link is valid. The LED on the top row indicates port speed. It will light solid green for 1000 Mbps connections, solid amber for 100 Mbps connections, and will remain off for 10 Mbps connections. A blinking green LED on the bottom row indicates packet activity on that port.

Switch to Hub or Switch

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

- A 10BASE-T hub or switch can be connected to the switch via a two-pair Category 3, 4, 5, or 5e UTP/STP cable.
- A 100BASE-TX hub or switch can be connected to the switch via a two-pair Category 5 or 5e UTP/STP cable.
- A 1000BASE-T switch can be connected to the switch via four-pair straight Category 5 or 5e UTP/STP cable.

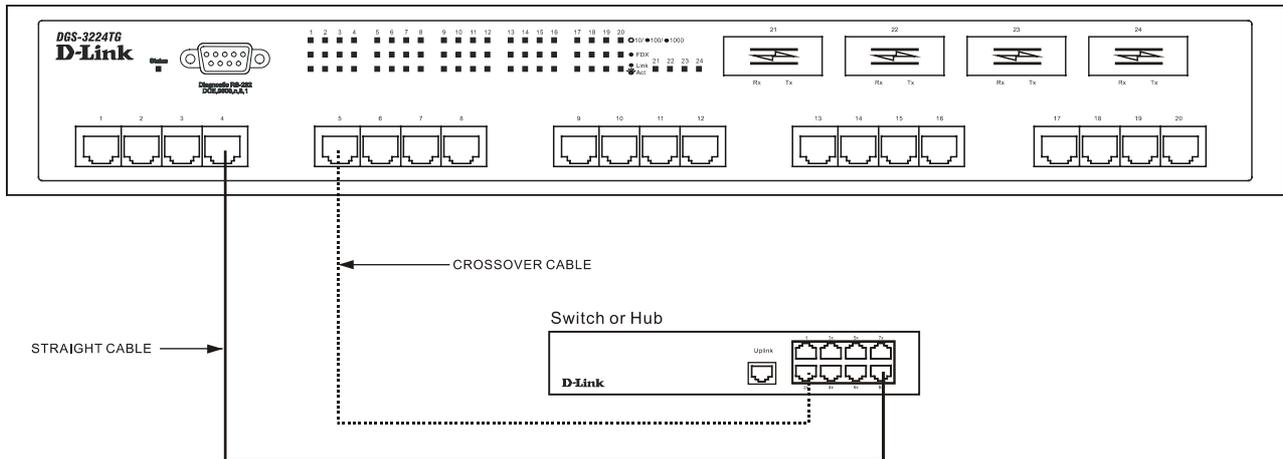


Figure 4-2. Switch connected to a normal (non-Uplink) port on a hub or switch using a straight or crossover cable

SWITCH MANAGEMENT AND OPERATING CONCEPTS

This chapter discusses many of the concepts and features used to manage the switch, as well as the concepts necessary for the user to understand the functioning of the switch. Further, this chapter explains many important points regarding these features.

Configuring the switch to implement these concepts and make use of its many features is discussed in detail in the next chapters.

Local Console Management

A local console is a terminal or a workstation running a terminal emulation program that is connected directly to the switch via the RS-232 console port on the front of the switch. A console connection is referred to as an 'Out-of-Band' connection, meaning that console is connected to the switch using a different circuit than that used for normal network communications. So, the console can be used to set up and manage the switch even if the network is down.

Local console management uses the terminal connection to operate the console program built-in to the switch (see Chapter 6, "*Using the Console Interface*"). A network administrator can manage, control and monitor the switch from the console program.

The DGS-3224TG contains a CPU, memory for data storage, flash memory for configuration data, operational programs, and SNMP agent firmware. These components allow the switch to be actively managed and monitored from either the console port or the network itself (out-of-band, or in-band).

Diagnostic (console) port (RS-232 DCE)

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) a to the RS-232 DCE console port of the switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management performed via management platforms, such as D-View, HP OpenView, etc.

The console port is set at the factory for the following configuration:

- Baud rate: 9,600
- Data width: 8 bits
- Parity: none
- Stop bits: 1
- Flow Control: None

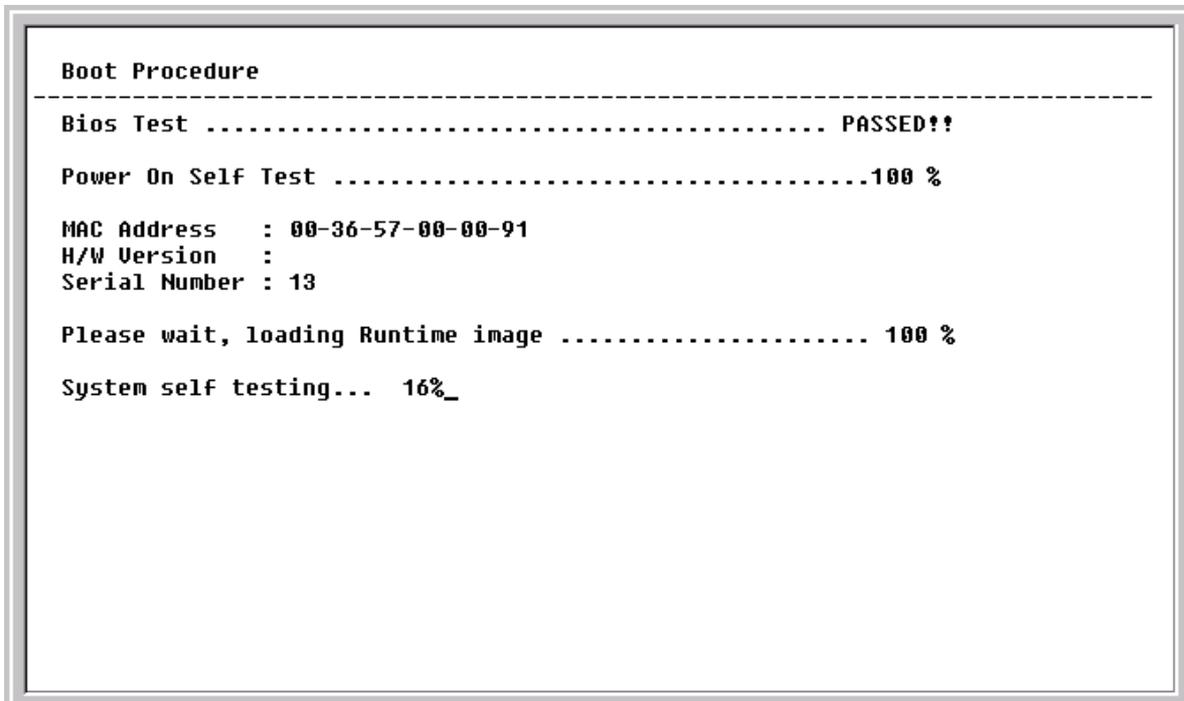
Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100. If you still don't see anything, try hitting <Ctrl> + r to refresh the screen.

IP Addresses and SNMP Community Names

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

The switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found from the initial boot console screen – shown below.



```
Boot Procedure
-----
Bios Test ..... PASSED!!

Power On Self Test .....100 %

MAC Address   : 00-36-57-00-00-91
H/W Version   :
Serial Number : 13

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

System self testing... 16%_
```

Figure 5-1. Boot Procedure screen

The switch's MAC address can also be found from the console program under the **Switch Information** menu item, as shown below.

```

Switch Information
-----
Device Type       : D-Link DGS-3224TG Ethernet Switch
MAC Address      : 00-36-57-00-00-91
Boot PROM Version : 0.00.002
Firmware Version  : 0.00.007
H/W Version      : 2A1

System Name       : [REDACTED]
System Location   : [REDACTED]
System Contact    : [REDACTED]

APPLY

ADVANCED SETTINGS
*****
Function:Sets a name for identification purposes.
Message:
CTRL+T = Root screen           Esc=Prev. screen           CTRL+R = Refresh

```

Figure 5-2. Switch Information menu

In addition, you can also set an IP address for a gateway router. This becomes necessary when the network management station is located on a different IP network from the switch, making it necessary for management packets to go through a router to reach the network manager, and vice-versa.

For security, you can set in the switch a list of IP Addresses of the network managers that allow you to manage the switch. You can also change the default SNMP Community Strings in the switch and set the access rights of these Community Strings. In addition, a VLAN may be designated as a Management VLAN.

Traps

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 recipient).

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

You can also specify which network managers may receive traps from the switch by entering a list of the IP addresses of authorized network managers. Up to four trap recipient IP addresses, and four corresponding SNMP community strings can be entered.

SNMP community strings function like passwords in that the community string entered for a given IP address must be used in the management station software, or a trap will be sent.

The following are trap types the switch can send to a trap recipient:

- **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 in that configuration settings saved to non-volatile RAM used to reconfigure the switch.

- **Authentication Failure** – This trap signifies that someone has tried to logon to the switch using an invalid SNMP community string. The switch automatically stores the source IP address of the unauthorized user.
- **New Root** – This trap indicates that the switch has become the new root of the Spanning Tree, the trap is sent by the switch 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 election as the new root.
- **Topology Change (STP)** – 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.

MIBs

Management and counter information are stored in the switch in the Management Information Base (MIB). The switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the switch also supports its own proprietary enterprise MIB as an extended Management Information Base. 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 port and type 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.

SNMP

The Simple Network Management Protocol (SNMP) is an OSI layer 7 (the application layer) protocol for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. SNMP can be used to perform many of the same functions as a directly connected console, or can be used within an integrated network management software package such as HP OpenView or DView.

SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol.

- Collecting information about the status and current configuration of network devices.
- Modifying the configuration of network devices.

The DGS-3224TG has a software program called an 'agent' that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

Authentication

The authentication protocol ensures that both the router SNMP agent and the remote user SNMP application program discard packets from unauthorized users. Authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the router SNMP must use the same community string. SNMP community strings of up to 20 characters may be entered under the **Remote Management Setup** menu of the console program.

Packet Forwarding

The switch enters the relationship between destination MAC or IP addresses and the Ethernet port or gateway router the destination resides on into its forwarding table. This information is then used to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only. Example: if Port 1 receives a packet destined for a station on Port 2, the switch transmits that packet through Port 2 only, and transmits nothing through the other ports. This process is referred to as 'learning' the network topology.

MAC Address Aging Time

The Aging Time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source and destination MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time.

The aging time can be from 17.2 to 2,200 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch.

If the Aging Time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Static forwarding entries are not affected by the aging time.

Filtering

The switch uses a filtering database to segment the network and control communication between segments. It can also filter packets off the network for intrusion control. Static filtering entries can be made by MAC Address filtering.

Each port on the switch is a unique collision domain and the switch filters (discards) packets whose destination lies on the same port as where it originated. This keeps local packets from disrupting communications on other parts of the network.

For intrusion control, whenever a switch encounters a packet originating from or destined to a MAC address entered into the filter table, the switch will discard the packet.

Some filtering is done automatically by the switch:

- Dynamic filtering – automatic learning and aging of MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.
- Filtering done by the Spanning Tree Protocol that can filter packets based on topology, making sure that signal loops don't occur.
- Filtering done for VLAN integrity. Packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3) will be filtered.

Spanning Tree Protocol

The IEEE 802.1D Spanning Tree Protocol allows for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically – without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

STP Operation Levels

STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier	A combination of the User-set priority and the switch's MAC	32768 + MAC

(Not configurable by setting below)	user- except priority	address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address	
Priority		A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time		The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer		Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer		The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

Table 5-1. STP Parameters – Switch Level

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	32768
Port Cost	A value used by STP to evaluate paths.	19

Table 5-2. STP Parameters – Port Group Level

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch

- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change. The goal is to make the fastest link the root port.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- Blocking – the port is blocked from forwarding or receiving packets
- Listening – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- Learning – the port is adding addresses to its forwarding database, but not yet forwarding packets
- Forwarding – the port is forwarding packets

- Disabled – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

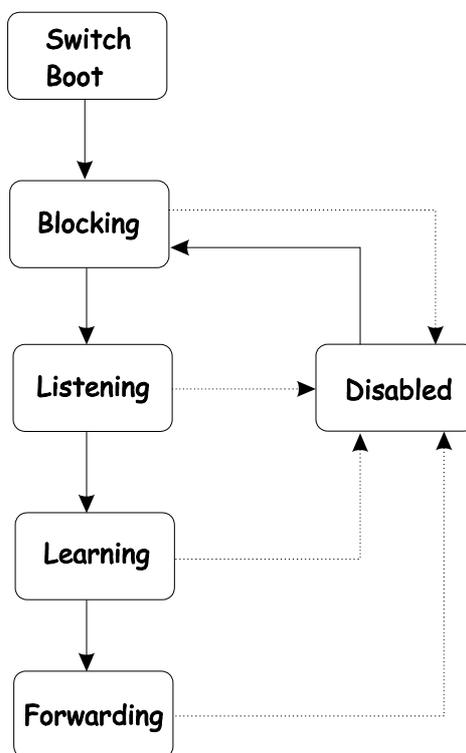


Figure 5-3. STP Port State Transitions

When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state.

No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP enabled for all ports
Port priority	128

Port cost	19
Bridge Priority	32,768

Table 5-3. Default STP Parameters

User-Changeable STP 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:

- **Priority** – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.
- **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: *The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.*

- **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.
- **Forward Delay Timer** – 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.

Note: *Observe the following formulas when setting the above parameters:*

$$\text{Max. Age} \leq 2 \times (\text{Forward Delay} - 1 \text{ second})$$

$$\text{Max. Age} \geq 2 \times (\text{Hello Time} + 1 \text{ second})$$

- **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.
- **Port Cost** – A Port Cost can be set from 1 to 65535. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP

A simple illustration of three Bridges (or three switches) connected in a loop is depicted in Figure 5-3. In this example, you can anticipate some major network problems if the STP assistance is not applied. If Bridge A broadcasts a packet to Bridge B, Bridge B will broadcast it to Bridge C, and Bridge C will broadcast it to back to Bridge A, and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure.

STP can be applied as shown in Figure 5-4. In this example, STP breaks the loop by blocking the connection between Bridge B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings. Now, if Bridge A broadcasts a packet to Bridge C, then Bridge C will drop the packet at port 2 and the broadcast will end there.

Setting-up STP using values other than the defaults can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the **Priority** setting, or influencing STP to choose a particular port to block using the **Port Priority** and **Port Cost** settings is, however, relatively straight forward.

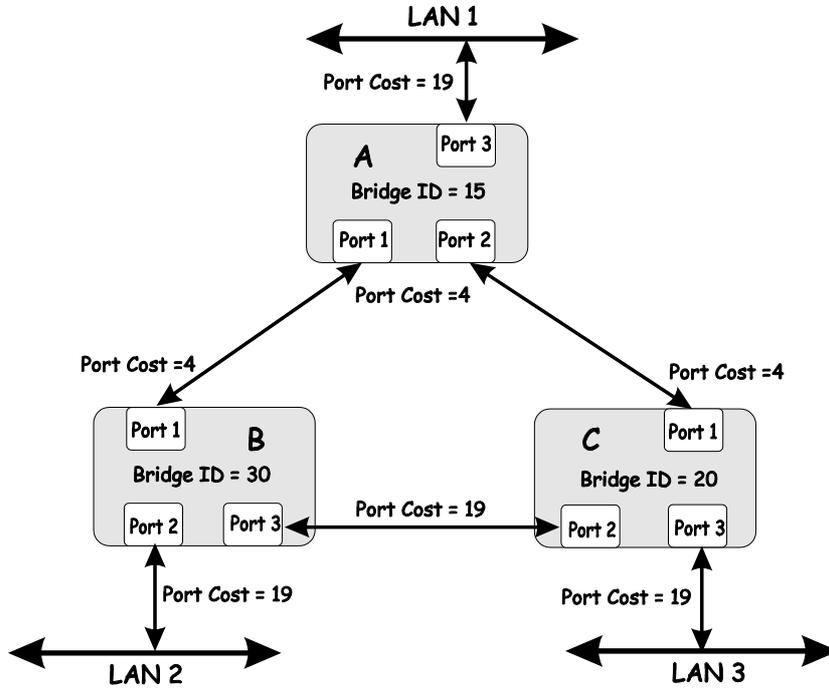


Figure 5-4. Before Applying the STA Rules

In this example, only the default STP values are used.

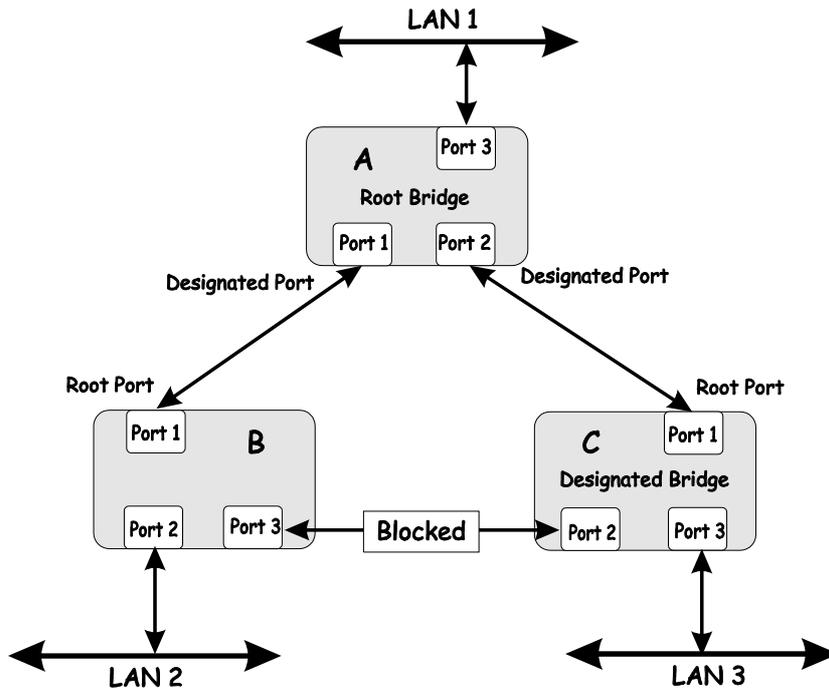


Figure 5-5. After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C.

Note also that the example network topology is intended to provide redundancy to protect the network against a link or port failure – not a switch failure or removal. For example, a failure of switch A would isolate LAN 1 from connecting to LAN 2 or LAN 3.

VLANs

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

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

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

Notes About VLANs on the DGS-3224TG

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets **cannot** cross VLANs without a network device performing a routing function between the VLANs.
2. The DGS-3224TG supports only IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
3. The switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN.
4. The DEFAULT_VLAN has a VID = 1.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** – A port on a switch where packets are flowing into the switch and VLAN decisions must be made.
- **Egress port** – A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the DGS-3224TG. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

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

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

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

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

The main characteristics of IEEE 802.1Q are as follows:

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

802.1Q VLAN Packet Forwarding

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

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

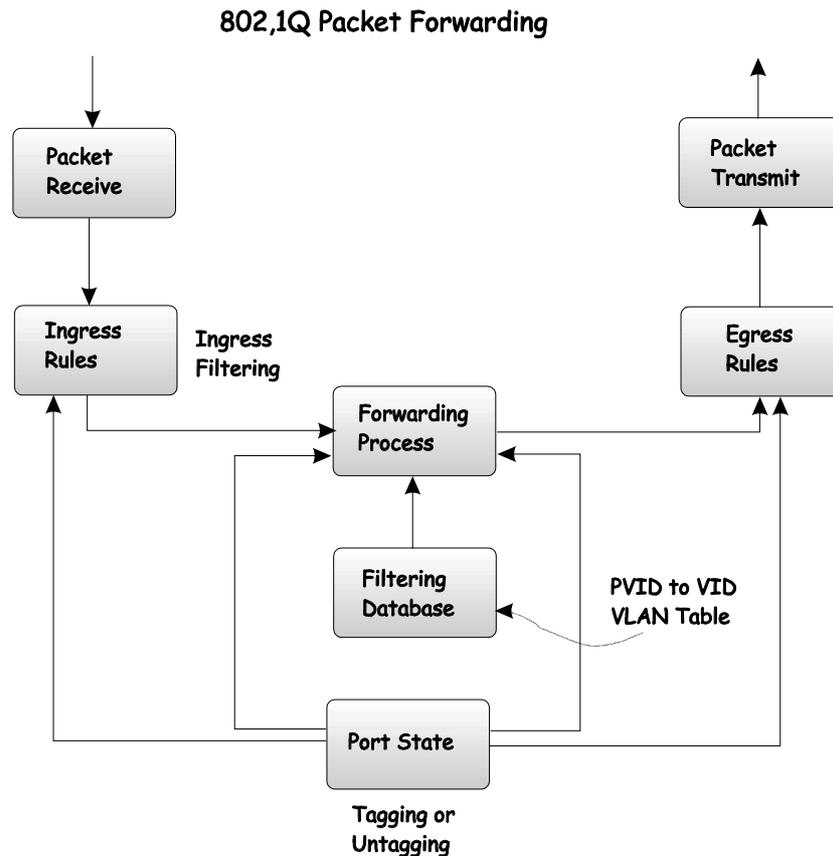


Figure 5-6. IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

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

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

destination address (found in the switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the switch will drop the packet.

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

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

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

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

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

Tagging and Untagging

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

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

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

Ingress Filtering

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

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

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

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

DHCP

The Dynamic Host Configuration Protocol (DHCP) can reduce the administrative burden of assigning and maintaining IP address information. DHCP provides reliable and simple TCP/IP network configuration, ensures that address conflicts do not occur, and helps to conserve the use of IP addresses through the centralized management of address allocation.

Dynamic address allocation enables a client to be assigned an IP address from a pool of free addresses. Each address is assigned with a lease and a lease expiration period. The client must renew the lease to continue using the assigned address. Dynamically assigned addresses can be returned to the free address pool if the computer is not being used, if it is moved to another subnet, or if its lease expires. Usually, network policy ensures that the same IP address is assigned to a client each time and that addresses returned to the free address pool are reassigned.

When the address lease expires, the DHCP client enters the renewing state. The client sends a request message to the DHCP server that provided the address. The DHCP server sends an acknowledgement that contains the new lease and configuration parameters. The client then updates its configuration values and returns to the bound state.

When the DHCP client is in the renewing state, it must release its address immediately in the rare event that the DHCP server sends a negative acknowledgment. The DHCP server sends this message to inform a client that it has incorrect configuration information, forcing it to release its current address and acquire new information.

If the DHCP client cannot successfully renew its lease, the client enters a rebinding state. The client then sends a request message to all DHCP servers in its range, attempting to renew its lease. Any DHCP server that can extend the lease sends an acknowledgement containing the extended lease and updated configuration information. If the lease expires or if a DHCP server responds with a negative acknowledgment, the client must release its current configuration, and then return to the initializing state.

If the DHCP client uses more than one network adapter to connect to multiple networks, this protocol is followed for each adapter that the user wants to configure for TCP/IP. Multi-homed systems are selectively configured for any combination of the system's interfaces.

When a DHCP-enabled computer is restarted, it sends a message to the DHCP server with its current configuration information. The DHCP server either confirms this configuration or sends a negative reply so that the client must begin the initializing state again. System startup might, therefore, result in a new IP address for a client computer, but neither the user nor the network administrator has to take any action in the configuration process.

Before loading TCP/IP with an address acquired from the DHCP server, DHCP clients check for an IP address conflict by sending an Address Resolution Protocol (ARP) request containing the address. If a conflict is found, TCP/IP does not start, and the user receives an error message. The conflicting address should be removed for the list of active leases or it should be excluded until the conflict is identified and resolved.

CONFIGURING THE SWITCH USING THE CONSOLE INTERFACE

Your 24-port 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 configure 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.

Notes are added where clarification is necessary.

Before You Start

The DGS-3224TG supports a wide array of functions and gives great flexibility and increased network performance by eliminating the routing bottleneck between the WAN or Internet and the Intranet. Its function in a network can be thought of as a new generation of router that performs routing functions in hardware, rather than software.

This flexibility and rich feature set requires a bit of thought to arrive at a deployment strategy that will maximize the potential of the switch.

Connecting to the Switch

You can use the console interface by connecting the switch to a VT100-compatible terminal or a computer running an ordinary terminal emulator program (e.g., the terminal program included with the Windows operating system) using an RS-232C serial cable. Your terminal parameters will need to be set to:

- VT-100/ANSI compatible
- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

You can also access the same functions over a Telnet interface. Once you have set an IP address for your switch, you can use a Telnet program (in VT-100 compatible terminal mode) to access and control the switch. All of the screens are identical, whether accessed from the console port or from a Telnet interface.

Console Usage Conventions

The console interface makes use of the following conventions:

1. Items in *<angle brackets>* can be toggled between several choices using the space bar.
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.
4. Items in **UPPERCASE** are commands. Moving the selection to a command and pressing Enter will execute that command, e.g. APPLY, etc.

Please note that the command APPLY only applies for the current session. Use **Save Changes** from the main menu for permanent changes. **Save Changes** enters the current switch configuration into non-volatile RAM, and then reboots the switch.

First Time Connecting to The Switch

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

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

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

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

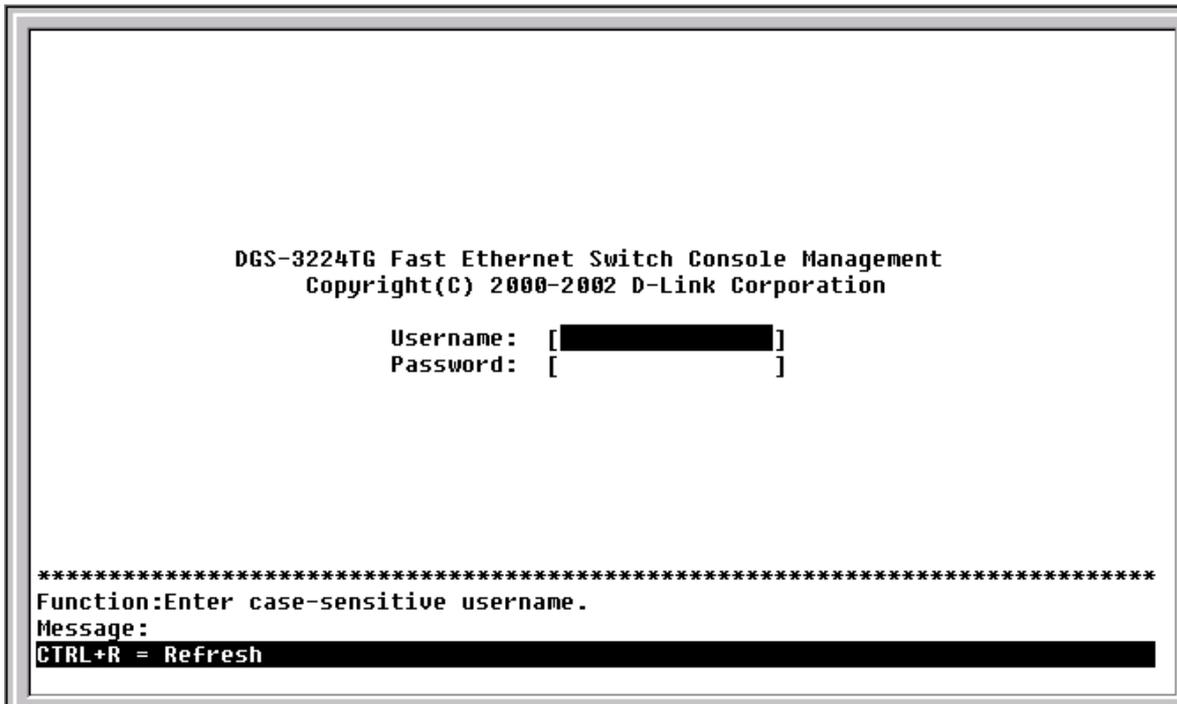


Figure 6-1. Initial screen, first time connecting to the switch

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

Press **Enter** in both the Username and Password fields. You will be given access to the main menu shown below:

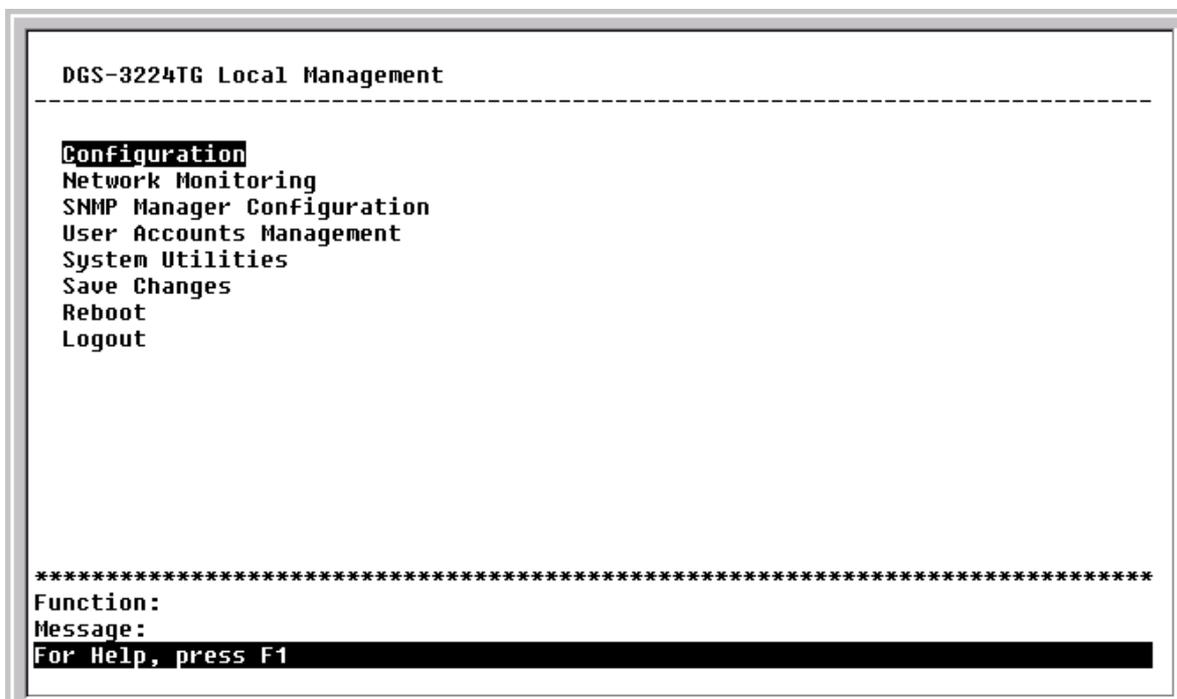


Figure 6-2. Main menu

Note: The first user automatically gets Root privileges (See Table 6-1). It is recommended to create at least one Root-level user for the switch.

User Accounts Management

To create a new user account, highlight **User Accounts Management** from the main menu and press **Enter**:

```

DGS-3224TG Local Management
-----

Configuration
Network Monitoring
SNMP Manager Configuration
User Accounts Management
System Utilities
Save Changes
Reboot
Logout

*****
Function:
Message:
For Help, press F1

```

Figure 6-3. Main menu

```

Setup User Accounts
-----

Action: <Add > Username: [          ]
New Password: [          ]
Confirm New Password: [          ]
Access Level: <Root > APPLY

-----

Current Accounts:      User Name      Access Level
                      -----

```

```

Function: Select action - ADD ,Delete or Update
Message:
CTRL+T = Root screen      Esc=Prev. screen      CTRL+R = Refresh

```

Figure 6-4. Setup User Accounts screen

From the main menu, highlight **User Accounts Management** and press **Enter**, then the **Setup User Accounts** screen appears.

1. Toggle the **Action** field to *<Add>* using the space bar. This will allow the addition of a new user. The other options are *<Delete>* - this allows the deletion of a user entry, and *<Update>* - this allows for changes to be made to an existing user entry.
2. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have *<Root>*, *<User+>*, or *<User>* privileges. The space bar toggles between the three options.
3. Highlight **APPLY** and press **Enter** to make the user addition effective.
4. Press **Esc.** to return to the previous screen or **Ctrl+T** to go to the root screen.
5. A listing of all user accounts and access levels is shown below the user setup menu. This list is updated when **APPLY** is executed.
6. Please remember that **APPLY** makes changes to the switch configuration for the **current session only**. All changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the main menu - if you want these changes to be permanent.

Root, User+ and Normal User Privileges

There are three levels of user privileges: *Root* and *User+*, and *User*. Some menu selections available to users with *Root* privileges may not be available to those with *User+* and *User* privileges.

The following table summarizes the *Root*, *User+* and *User* privileges:

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

Table 6-1. Root, User+, and User Privileges

After establishing a User Account with **Root**-level privileges, press **Esc.** Then highlight **Save Changes** and press **Enter** (see below). The Switch will save any changes to its non-volatile ram and reboot. You can logon again and are now ready to continue configuring the Switch.

Save Changes

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

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

To retain any configuration changes permanently, highlight **Save Changes** from the main menu.

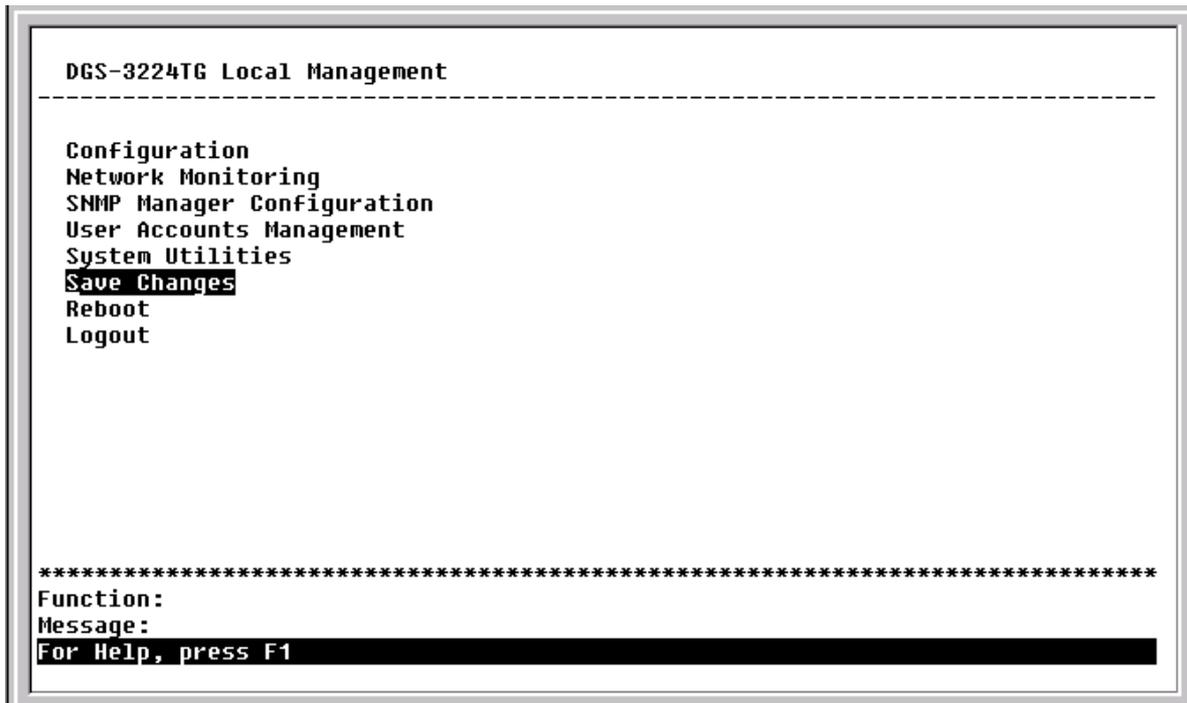


Figure 6-5. Main menu

The following screen will appear to verify that your new settings have been saved to NV-RAM:

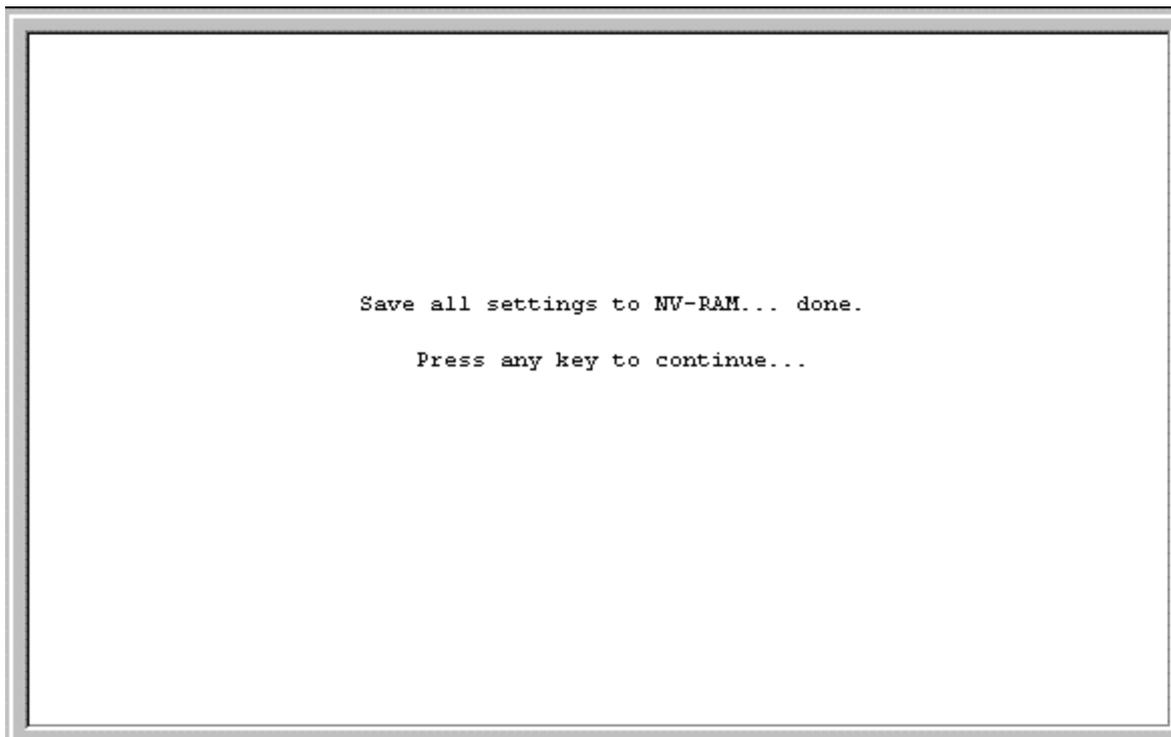


Figure 6-6. Save changes screen

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

Factory Reset

The only way to change the configuration stored in NV-RAM is to save a new configuration using **Save Changes**, or to execute a **Load Factory Default Configuration** from the **System Reboot** menu (under **Reboot** on the main menu). This will clear all settings and restore them to their initial values listed in the appendix. These are the configuration settings entered at the factory and are the same settings present when the switch was purchased.

```

DGS-3224TG Local Management
-----

Configuration
Network Monitoring
SNMP Manager Configuration
User Accounts Management
System Utilities
Save Changes
Reboot
Logout

*****
Function:
Message:
For Help, press F1

```

Figure 6-7. Main menu

Highlight **Reboot** from the main menu and press **Enter**.

```

System Reboot
-----

Reboot

Save Configuration & Reboot

Reboot & Load Factory Default Configuration

Reboot & Load Factory Default Configuration Except IP Address

*****
Function:
Message:
CTRL+T = Root screen           Esc=Prev. screen           CTRL+R = Refresh

```

Figure 6-8. System Reboot menu

Highlight the appropriate choice and press **Enter** to reset the switch's NV-RAM to the factory default settings (or just reboot the switch). Loading the Factory Default Configuration will erase any User Accounts (and all other configuration settings) you may have entered and return the switch to the state it was in when it was

purchased. The **Load Factory Default Configuration Except IP Address** option is used when the switch will be managed by the Telnet manager, which requires knowledge of the switch's IP address to function.

Logging Onto The Switch Console

To log in once you have created a registered user, from the login screen:

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 access level or privilege.

Updating or Deleting User Accounts

To update or delete a user password:

Choose **User Accounts Management** from the main menu. The following **Setup User Accounts** screen appears:

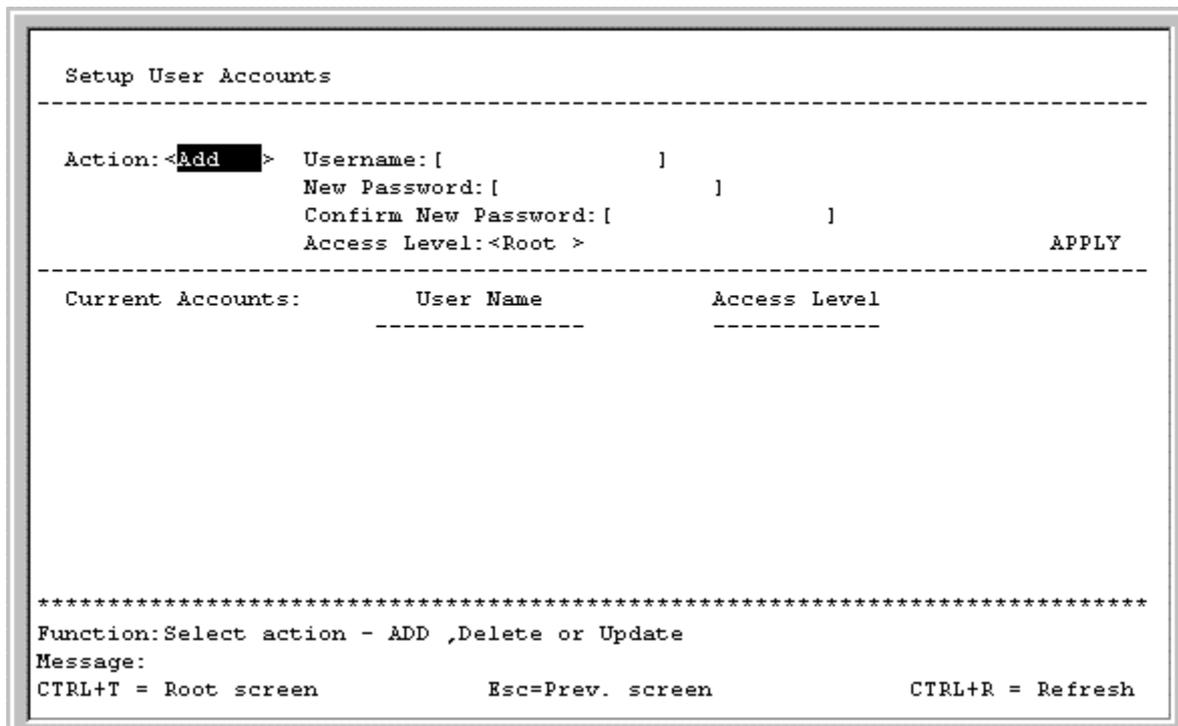


Figure 6-9. Setup User Accounts screen

1. Toggle the **Action** field using the space bar to choose *Add*, *Update*, or *Delete*.
2. Type in the **Username** for the user account you wish to change.
3. You can now modify the password or the privilege level for this user account.
4. If the password is to be changed, 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.

5. If the privilege level is to be changed, toggle the **Access Level** field until the appropriate level is displayed – *Root*, *User+* or *User*.
6. Highlight APPLY and press **Enter** to make the change effective.
7. You must enter the configuration changes into the non-volatile ram (NV-RAM) using **Save Changes** from the main menu if you want the configuration to be used after a switch reboot.

Only a user with **Root** privileges can make changes to user accounts.

Viewing Current User Accounts

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

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

To view the current user accounts, highlight **User Accounts Management** from the main menu. The current user accounts can be read from the **Setup User Accounts** screen.

Deleting a User Account

1. Toggle the **Action** field to **Delete**.
2. Enter the **Username** for the account you want to delete. You must enter the password for the account to be able to delete it.
3. Highlight APPLY and press **Enter** to make the deletion of the selected user take effect.
4. You must enter the configuration changes into the non-volatile ram (NV-RAM) using **Save Changes** from the main menu if you want the configuration to be used after a switch reboot.

Only users with root privileges can delete user accounts.

Configuration

This section will help prepare the switch user by describing the **Remote Management Setup**, **Switch Information**, **Configure Advanced Switch Features**, **Configure Ports**, **Configure Spanning Tree**, **Port Spanning Tree Settings**, **Setup Unicast Forwarding Table**, **Setup Static Multicast Forwarding Table**, **IEEE 802.1Q VLANs Configuration**, **802.1Q Static VLAN Settings**, **Port VLAN assignment**, **Ingress Filter Settings**, **Port GVRP Settings**, **IGMP Snooping Settings**, **Link Aggregation**, **Setup Port Mirroring**, **Class of Service Configuration**, **Port Default Priority assignment**, **Traffic Class Configuration**, and **Serial Port and SLIP Settings** screens, all of which can be found under the **Configuration** menu, along with various submenus.

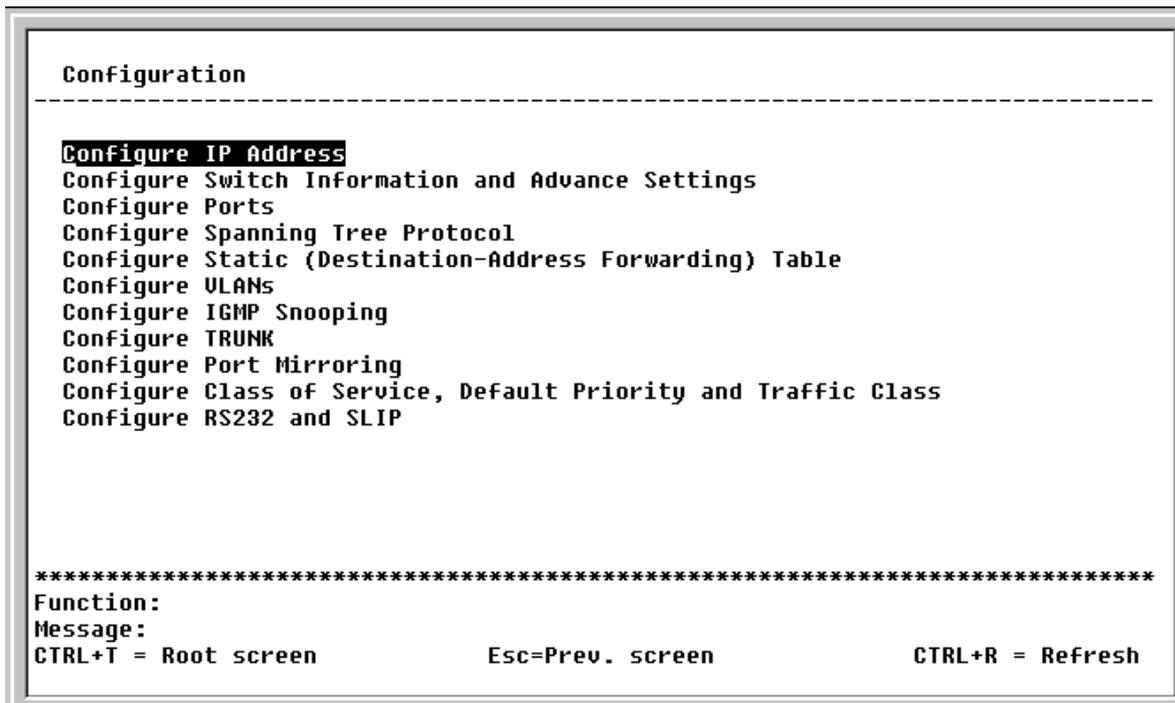


Figure 6-10. Configuration menu

Configure IP Address

Some settings must be entered to allow the switch to be managed from an SNMP-based Network Management System such as SNMP v1 or to be able to access the switch using the Telnet protocol.

The **Remote Management Setup** screen lets you specify how the switch will be assigned an IP address to allow the switch to be identified on the network.

To setup the switch for remote management, highlight **Configure IP Address** from the **Configuration** menu. The following screen appears:

```

Remote Management Setup
-----

Current Switch IP Settings:

  Get IP From:      Manual
  IP Address:       10.24.22.3
  Subnet Mask:      255.0.0.0
  Default Gateway: 10.254.254.251
  Management VID:   1

New Switch IP Settings:

  Get IP From:      <Manual >
  IP Address:       [10.24.22.3   ]
  Subnet Mask:      [255.0.0.0   ]
  Default Gateway: [10.254.254.251]
  Management VID:   [1     ]

                                APPLY

*****
Function:Apply the settings.
Message: All changes applied!
CTRL+T = Root screen           Esc=Prev. screen           CTRL+R = Refresh

```

Figure 6-11. Remote Management Setup screen

The switch needs to have an IP address assigned to it so that an in-band network management system (e.g. Telnet) client can find it on the network. The **Remote Management Setup** screen allows you to change the settings for the two different management 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. Please see the *Configure RS232 and SLIP* section later in this manual for further information.

The fields listed under the **Current Switch IP Settings** heading are those currently being used by the switch. Those fields listed under the **New Switch IP Settings** heading are those that will be used after the switch has been rebooted.

Toggle the **Get IP From** field using the space bar to choose from *Manual*, *BOOTP*, or *DHCP*. This selects how the switch will be assigned an IP address on the next reboot (or startup).

The **Get IP From** options are:

- *BOOTP* – The switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
- *DHCP* – The switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
- *Manual* – Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the switch. These fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields which require entries under this option are as follows:

- **IP Address** – Determines the IP address used by the switch for receiving SNMP and Telnet communications. These fields 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** – A bitmask that determines the extent of the subnet that the switch is on. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
- **Default Gateway** – IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the switch to be accessible outside your local network, you can leave this field unchanged.
- **Management VID:[]** – Allows the entry of the VLAN ID (VID) of a VLAN that will have access to the Telnet manager. This will be the VID of the VLAN that a management station is located on.

Configure Switch Information and Advanced Settings

Highlight **Configure Switch Information and Advanced Settings** on the **Configuration** menu and press **Enter**:

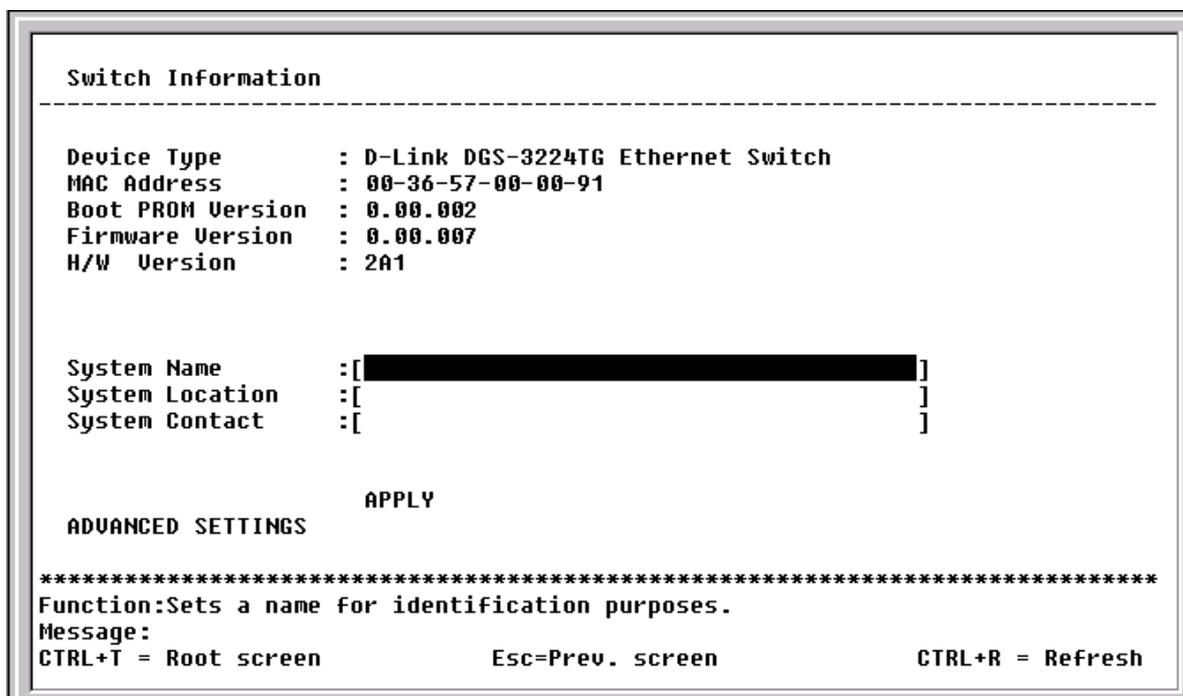


Figure 6-12. Switch Information menu

The **Switch Information** shows the type of switch and its **MAC Address** (assigned by the factory and unchangeable). In addition, the **Boot PROM Version**, **Firmware Version**, and hardware version numbers are shown. This information is helpful to keep track of PROM and firmware updates and to obtain the switch's MAC address for entry into another network device's address table – if necessary.

You can also enter the name of the **System**, its location, and the name and telephone number of the system administrator. It is recommended that the person responsible for the maintenance of the network system that this switch is installed on be listed here.

Configure Advanced Switch Features

Select **ADVANCED SETTINGS** at the bottom of the **Switch Information** menu and press **Enter** to access the following **Configure Advanced Switch Features** menu:

```

Configure Advanced Switch Features
-----
Auto-Logout:<Never >
MAC Address Aging Time(sec):[300  ]
IGMP Snooping:<Disabled>
Switch GURP:<Enabled >
Scheduling Mechanism for CoS Queues:<Strict  >
Trunk Load Sharing Algorithm: <Src Address  >

      APPLY

REALCLOCK SETTINGS

*****
Function:Select auto logout timer.
Message:
CTRL+T = Root screen           Esc=Prev. screen           CTRL+R = Refresh

```

Figure 6-13. Configure Advanced Switch Features menu

This screen allows you to set the following features:

- **Auto-Logout:<Never>** – This sets the time the interface can be idle before the switch automatically logs-out the user. The options are *2 mins*, *5 mins*, *10 mins*, *15 mins*, or *Never*.
- **MAC Address Aging Time (sec):[300]** – This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between 17 and 2200 seconds.

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

- **IGMP Snooping:<Disabled>** – This setting enables Internet Group Management Protocol (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).
- **Switch GVRP:<Disabled>** – Group VLAN Registration Protocol is a protocol that allows members to dynamically join VLANs. This is used to enable or disable GVRP on the switch.

- **Scheduling Mechanism for CoS Queues:**<Strict> – There are two Class of Service queue options, *RoundRobin* and *Strict*. If *Strict* is selected, when the highest priority queue is full, those packets will be the first to be forwarded. If *RoundRobin* is selected, the forwarding is based on the settings made on the **Class of Service Configuration** screen.
- **Trunk Load Sharing Algorithm:**<Src Address> – The trunk load sharing options are *Dst Address*, *Src&Dst Address*, and *Src Address*.

In addition, clicking REALCLOCK SETTINGS at the bottom of the **Configure Advanced Switch Features** menu will allow you to configure the Real-time Clock for network monitoring and troubleshooting purposes.

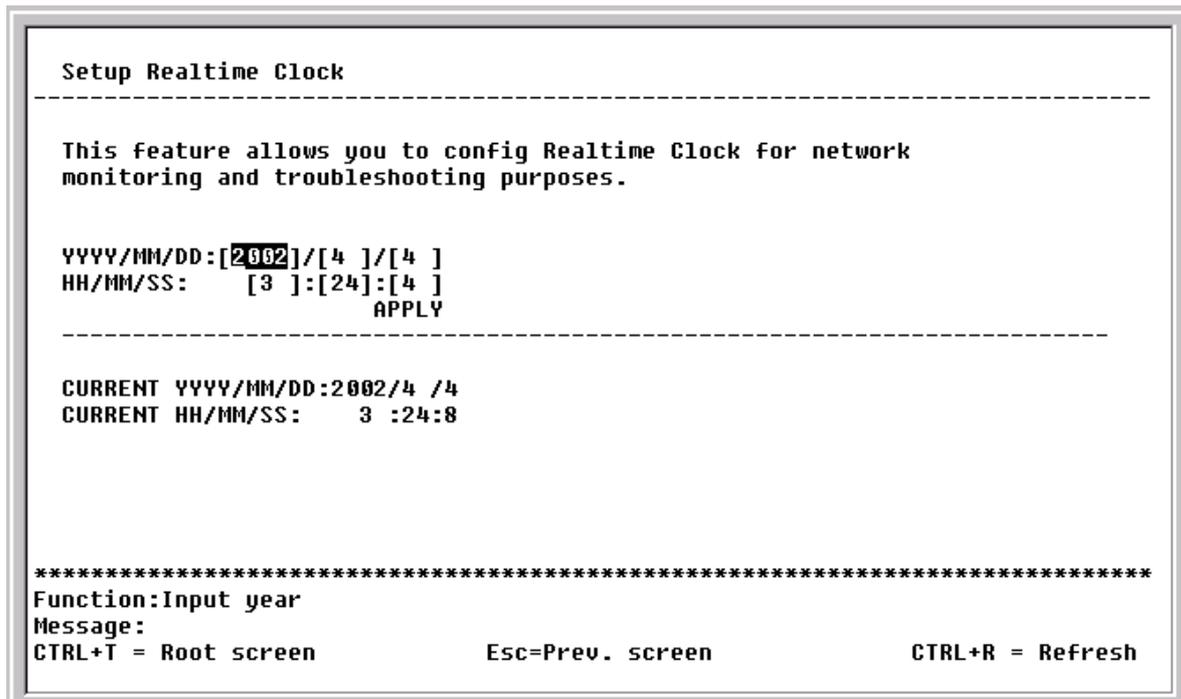


Figure 6-14. Setup Realtime Clock screen

Configure Ports

Highlight **Configure Ports** from the **Configuration** menu and press **Enter**:

```

Configure Ports
-----
View Ports:<1 to 12 >          Configure Port from [1 ] to [1 ]
State:<Enabled > Speed/Duplex:<Auto > Flow Control: Auto          APPLY
-----
Port      State      Settings      Connection      Port type
-----
1         Enabled   Auto/Enabled  100M/Full/None  1000TX
2         Enabled   Auto/Enabled  -               1000TX
3         Enabled   Auto/Enabled  -               1000TX
4         Enabled   Auto/Enabled  -               1000TX
5         Enabled   Auto/Enabled  -               1000TX
6         Enabled   Auto/Enabled  -               1000TX
7         Enabled   Auto/Enabled  -               1000TX
8         Enabled   Auto/Enabled  -               1000TX
9         Enabled   Auto/Enabled  -               1000TX
10        Enabled   Auto/Enabled  -               1000TX
11        Enabled   Auto/Enabled  -               1000TX
12        Enabled   Auto/Enabled  -               1000TX
*****
Function:Select the scope of ports for display and configuration.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh

```

Figure 6-15. Configure Ports screen

Toggle the **View Ports** field, using the space bar, to view the configuration of either ports 1 through 12, 13 through 20, or 21 through 24. To configure a specific port, toggle the **Configure Port from [] to []** field until the appropriate port number or port range appears.

Toggle the **State** field to either enable or disable a given port.

Toggle the **Speed/Duplex** field to select the speed and duplex/half-duplex state of the ports *1x* to *20x*. *Auto* means auto-negotiation between 10, 100, and 1000 Mbps devices, in full- or half-duplex mode. The *Auto* setting allows the twenty copper ports to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *100M/Full*, *100M/Half*, *10M/Full*, *10M/Half*. There is no automatic adjustment of port settings with any option other than *Auto*. **Flow Control** can be enabled or disabled manually when any setting other than *Auto* is selected. Please note that the switch's four GBIC ports only support *1000M/Full*.

Configure Spanning Tree Protocol

To globally configure STP on the Switch, highlight **Configure Spanning Tree Protocol** on the **Configuration** menu and press **Enter**:

```

Configure Spanning Tree
-----
Switch Settings:
  Status: <Disabled>
  Max Age: [20]
  Hello Time: [2 ]
  Forward Delay: [15]
  Priority: [32768]
  APPLY

Port Settings

*****
Function:Set spanning tree status.
Message:
CTRL+T = Root screen           Esc=Prev. screen           CTRL+R = Refresh

```

Figure 6-16. Configure Spanning Tree menu

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

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

The user-changeable parameters in the Switch are as follows:

- **Status:** <Disabled> – Toggle to *Enabled* to implement the Spanning Tree Protocol on the switch.
- **Max Age:** [20] – The Maximum Age can be set from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge.
- **Hello Time:** [2] – The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. 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: *The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.*

- **Forward Delay:** [15] – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.
- **Priority:** [32768] – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch.

Note: Observe the following formulas when setting the above parameters:

Max. Age $\leq 2 \times$ (Forward Delay - 1 second)

Max. Age $\geq 2 \times$ (Hello Time + 1 second)

Port Spanning Tree Settings

In addition to setting Spanning Tree parameters for use on the switch level, the DGS-3224TG allows for the configuration of Spanning Tree Protocol on individual ports.

To define individual ports, highlight **Port Settings** on the **Configure Spanning Tree** menu above and press **Enter**.

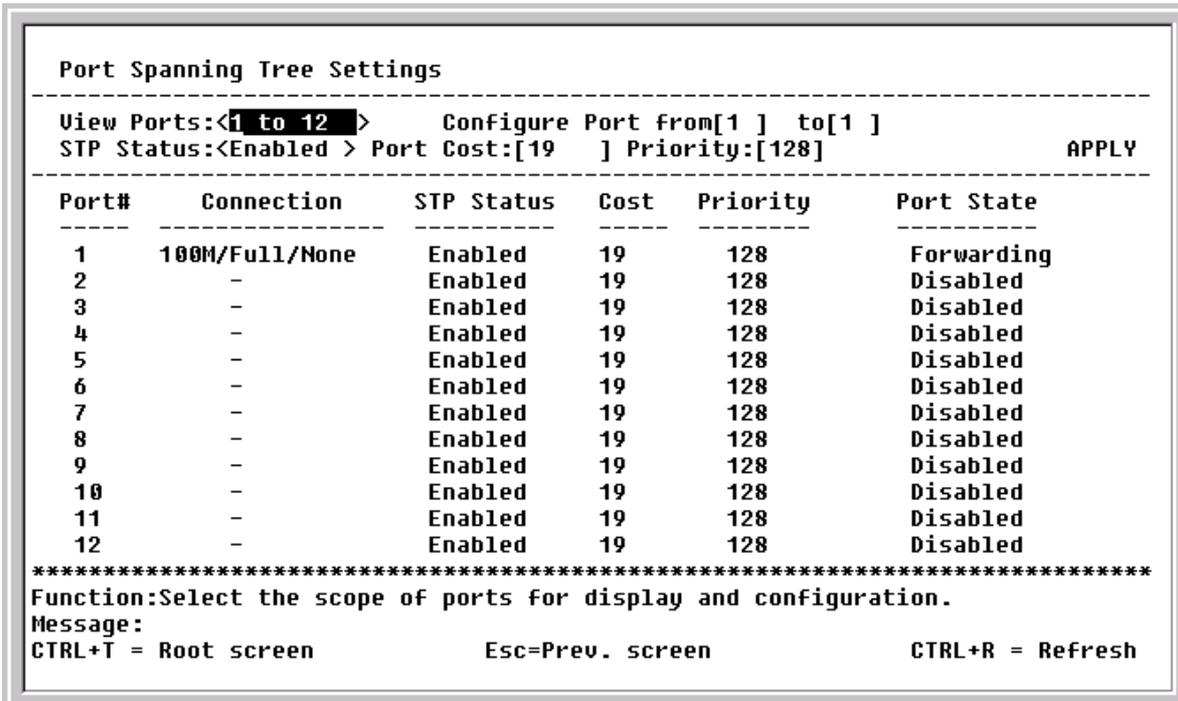


Figure 6-17. Port Spanning Tree Settings screen

Toggle the **View Ports** field to the range of ports to be configured. Enter the port number or port range in the **Configure Port from [] to []** field. After enabling or disabling **STP Status**, you can set the spanning tree port cost and priority.

Configure Static (Destination-Address Forwarding) Table

The **Configure Static (Destination-Address Forwarding) Table** menu allows you to access screens to create, modify, and delete both Static Unicast Forwarding Table and Static Multicast Forwarding Table entries, respectively.

Highlight **Configure Static (Destination-Address Forwarding) Table** on the **Configuration** menu and press **Enter**:

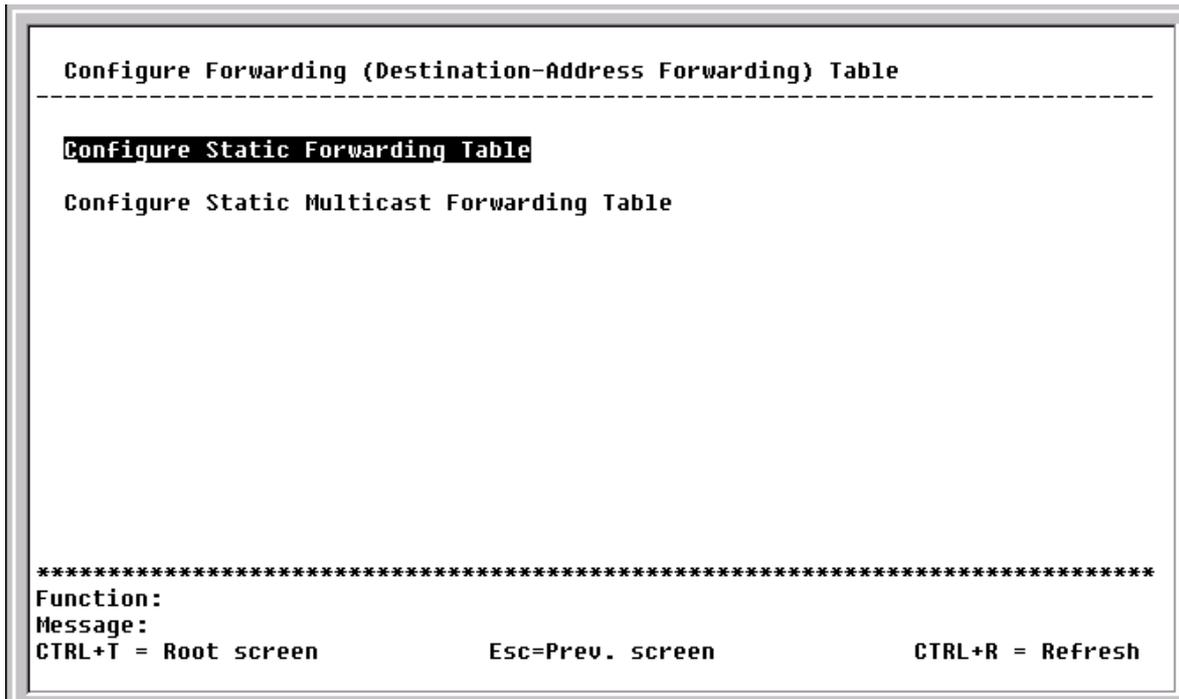


Figure 6-18. Configure Static (Destination-Address Forwarding) Table menu

Setup Unicast Forwarding Table

Highlight **Configure Static Forwarding Table** on the menu above to access the following screen:

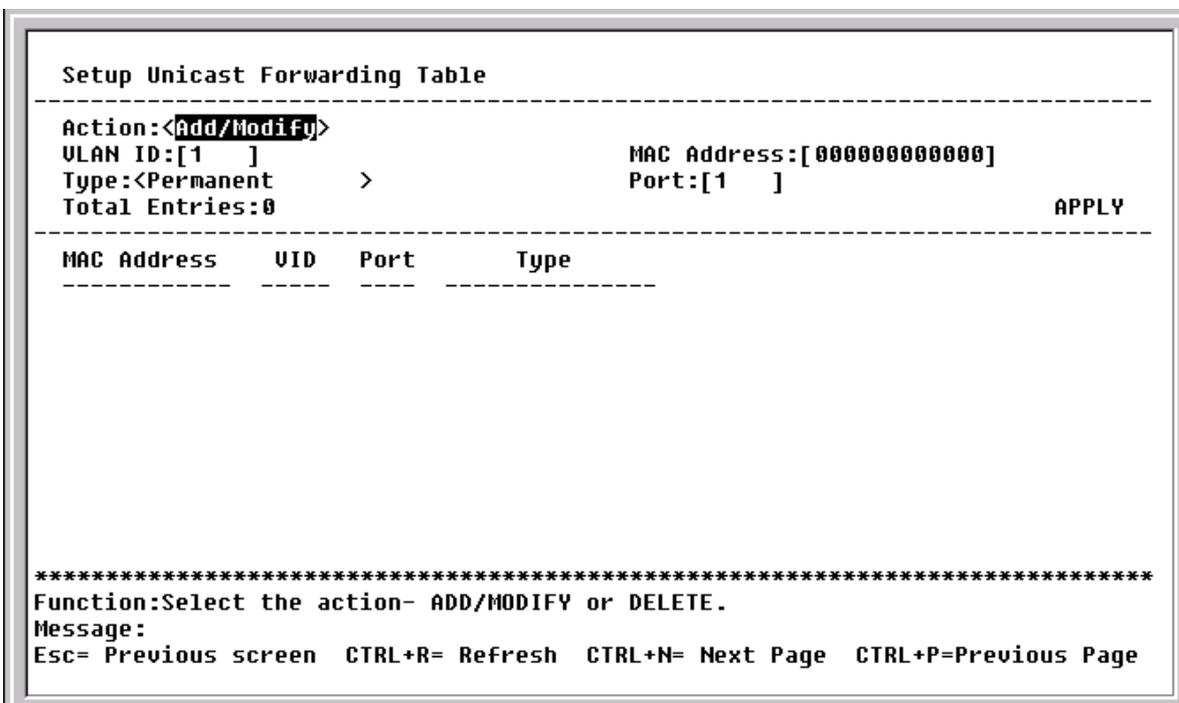


Figure 6-19. Setup Unicast Forwarding Table screen

The **Action** field can be toggled between *Add/Modify* and *Delete* using the space bar. Enter the VID in the **VLAN ID** field and the MAC address to be statically entered in the forwarding table in the **MAC**

Address field. There are two static unicast forwarding types to select from, *Permanent* and *DeleteOnReset*. Enter the port number in the **Port** field.

Highlight **APPLY** and press **Enter** to make the changes current. Use **Save Changes** from the main menu to enter the changes into NV-RAM.

Setup Static Multicast Forwarding Table

To edit the IEEE 802.1q Multicast Filtering settings, highlight **Configure Static Multicast Forwarding Table** on the **Configure Static (Destination-Address Forwarding) Table** menu above to access the following screen:

```

Setup Static Multicast Forwarding Table
-----
Action: <Add/Modify>      VLAN ID:[1 ]
Multicast MAC Address:[000000000000]
Port  1 to 8 9 to 16 17 to 20 21 to 24
(E/-) [-----][-----][----] [----]
Type:<Permanent      >                               Total Entries:0      APPLY
-----
MAC Address  VID  1 to 8 9 to 16 17 to 20 21 to 24      Type
-----
*****
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page

```

Figure 6-20. Setup Static Multicast Forwarding Table screen

The **Action** field can be toggled between *Add/Modify* and *Delete* using the space bar. To add a new entry to the static multicast forwarding table, select *Add/Modify* and enter the VLAN ID number of the VLAN that will be receiving the multicast packets. Enter the MAC address of the multicast source, and then enter the member ports. Each port can be either Egress or a non-member of the multicast group, on a per-VLAN basis. There are two static multicast forwarding types to select from, *Permanent* and *DeleteOnReset*.

To set a port's multicast group membership status, highlight the first field of **(E/-)**. Each port's multicast group membership can be set individually by highlighting the port's entry using the arrow keys, and then toggling between *E* and *-* using the space bar.

- *E* (Egress Member) – Specifies the port as being a static member of the multicast group. Egress Member Ports are ports that will be transmitting traffic for the multicast group.
- *-* (Non-Member) – Specifies the port as not being a member of the multicast group, but the port can become a member of the multicast group dynamically.

Highlight **APPLY** and press **Enter** to make the changes current. Use **Save Changes** from the main menu to enter the changes into NV-RAM.

Note: The DGS-3224TG supports a maximum of 16K multicast MAC address entities.

Configure VLANs

The switch reserves one VLAN, VID = 1, called the DEFAULT_VLAN for internal use. The factory default setting assigns all ports on the switch to the DEFAULT_VLAN. As new VLANs are configured, their respective member ports are removed from the DEFAULT_VLAN. If the DEFAULT_VLAN is reconfigured, all ports are again assigned to it. Ports that are not wanted as part of the DEFAULT_VLAN are removed during the configuration.

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

Note: The switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLANs are created, the member ports assigned to the new VLAN will be removed from the default VLAN port member list.

Note: The DEFAULT_VLAN has a VID = 1. An IP interface called System in the IP interface entry menu also has a VID = 1, and therefore corresponds to the DEFAULT_VLAN.

To create a new 802.1Q VLAN:

The VLAN menu adds an entry to edit the VLAN definitions and to configure the port settings for IEEE 802.1Q VLAN support. Highlight **Configure VLANs** from the **Configuration** menu and press **Enter**.

```

IEEE 802.1Q VLANs Configuration
-----
Configure Static VLAN Entry
Configure Port VLAN ID
Configure Port Ingress Filter
Configure Port GVRP Settings

*****
Function:
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh

```

Figure 6-21. IEEE 802.1Q VLANs Configuration menu

802.1Q Static VLAN Settings

To create an 802.1Q VLAN, highlight **Configure Static VLAN Entry** and press **Enter**:

```

802.1Q Static VLAN Settings
-----
VID: [2]      VLAN Name:[          ]      Entries: 1
          1      8 9      16 17 20      21 24
Egress/Forbidden:[-----][-----][----]  [----]
Tag/Untag       :[UUUUUUUU][UUUUUUUU][UUUU]  [UUUU]
State           :<Active >      APPLY
-----

VID      VLAN Name      Port List-Egress/Forbidden,Tag/Untag
1        DEFAULT_VLAN  EEEEEEEE EEEEEEEE EEEEEEEE
                        UUUUUUUU  UUUUUUUU  UUUUUUUU

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

```

Figure 6-22. 802.1Q Static VLAN Settings screen

To create an 802.1Q VLAN, enter a VLAN ID number in the **VID** field and a name for the new VLAN in the **VLAN Name** field.

To set the 802.1Q VLAN membership status of a port:

To enter the 802.1Q VLAN status for a port, highlight the first field of **Egress/Forbidden**. Each port's 802.1Q VLAN membership can be set individually by highlighting the port's entry using the arrow keys, and then toggling among *E*, *F*, and *-* using the space bar.

- *E* (Egress Member) – Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
- *F* (Forbidden Non-Member) – Defines the port as a non-member and also forbids the port from joining a VLAN dynamically.
- *-* (Non-Member) – Specifies the port as not being a member of the VLAN, but the port can become a member of the VLAN dynamically.

Next, determine which of the ports that are members of the new VLAN will be Tagged or Untagged ports.

To set a port as either a Tagged or an Untagged port:

Highlight the first field of **Tag/Untag** field. Each port's state can be set by highlighting the port's entry using the arrow keys and then toggling between U or T using the space bar.

- *U* - specifies the port as an Untagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.
- *T* - specifies the port as a Tagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated

with the PVID (Port VLAN Identifier – see below). When a tagged packet exits the port, the packet header is unchanged.

If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), then the port should be set to U – Untagged.

If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), then the port should be set to T – Tagged.

Once you have toggled between *Active* and *Inactive* under **State**, press APPLY to make the additions or deletions effective for the current session. To enter the changes into Non-volatile RAM, highlight **Save Changes** from the main menu and press **Enter**.

Port VLAN assignment

To assign a port a PVID, highlight **Configure Port VLAN ID** on the **IEEE 802.1Q VLANs Configuration** menu and press **Enter**:

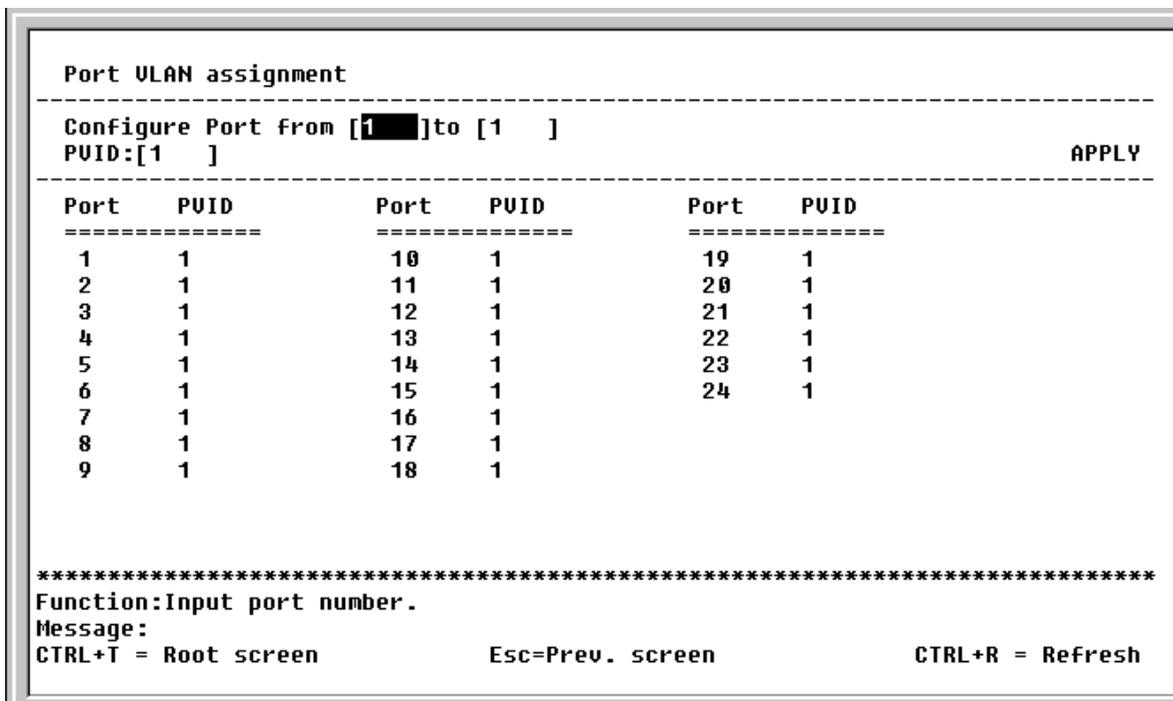


Figure 6-23. Port VLAN assignment screen

Highlight the **Configure Port from [1] to [1]** field and enter the range of port numbers you want to configure. Next, highlight the **PVID** field and enter the PVID for the VLAN's member ports you want to configure.

Port VLAN Identifier (PVID) is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the **802.1Q Static VLAN Settings** screen above.

Ingress Filter Settings

To set ingress filtering on a port, highlight **Configure Port Ingress Filter** on the **IEEE 802.1Q VLANs Configuration** menu and press **Enter**:

```

Ingress Filter Settings
-----
Configure Port from [1] to [1 ]
Ingress Filter:<Off >                                     APPLY
-----
Port  Ingress      Port  Ingress      Port  Ingress
-----
 1     Off          10     Off          19     Off
 2     Off          11     Off          20     Off
 3     Off          12     Off          21     Off
 4     Off          13     Off          22     Off
 5     Off          14     Off          23     Off
 6     Off          15     Off          24     Off
 7     Off          16     Off
 8     Off          17     Off
 9     Off          18     Off

*****
Function:Input port number.
Message:
CTRL+T = Root screen           Esc=Prev. screen           CTRL+R = Refresh

```

Figure 6-24. Ingress Filter Settings screen

Highlight the **Configure Port from [1] to [1]** field and enter the range of port numbers you want to configure. Then use the space bar to toggle between *On* and *Off* in the **Ingress Filter** field.

An Ingress Filter enables the port to compare the VID tag of an incoming packet with the both the VIDs and PVIDs of VLANs assigned to the port. If the VID tag of an incoming port is different from either the VID or PVID assigned to the port, the port filters (drops) the packet.

Port GVRP Settings

GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q ports.

To enable a port to dynamically become a member of a VLAN, highlight **Configure Port GVRP Settings** on the **IEEE 802.1Q VLANs Configuration** menu and press **Enter**:

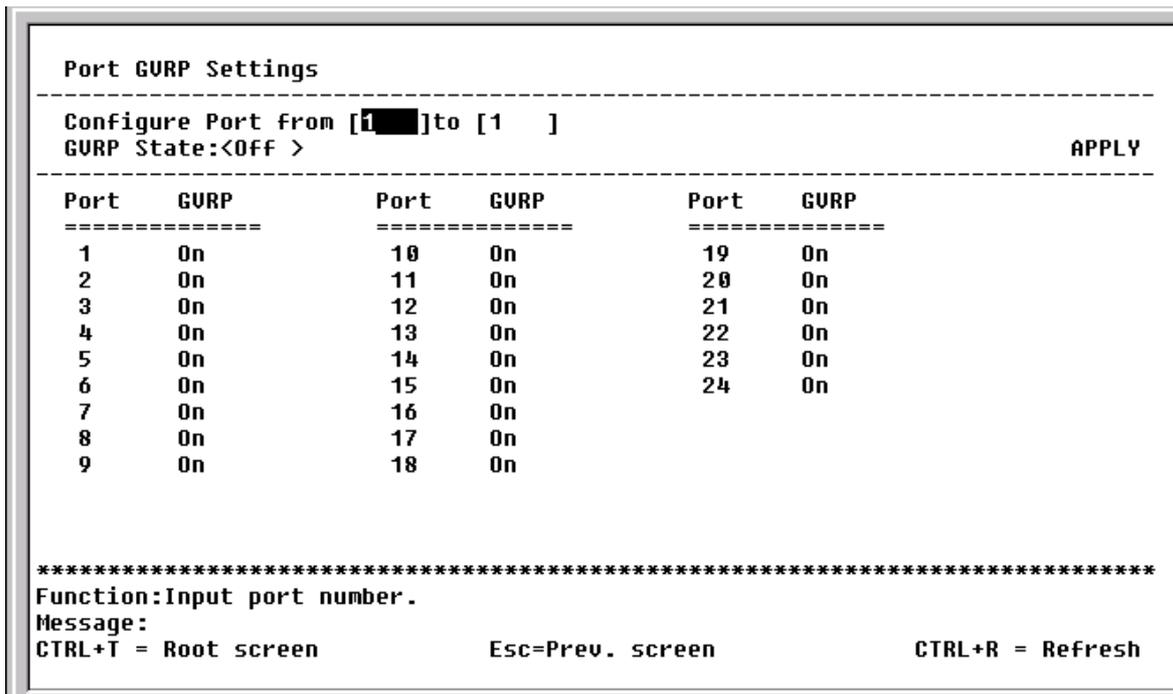


Figure 6-25. Port GVRP Settings screen

This screen allows you to enable or disable GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol, on individual ports. Enter the range of ports to be configured in the first two fields and then toggle the GVRP State to *On*. Press APPLY to let your changes take effect.

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.

Configure IGMP Snooping

IGMP Snooping can be globally enabled or disabled from the **IGMP Snooping Settings** screen.

To configure IGMP Snooping, highlight **Configure IGMP Snooping** on the **Configuration** menu and press **Enter**.

```

IGMP Snooping Settings
-----
Switch IGMP Snooping: Disabled
*Notes: If you want to change it, back to Configure Switch.
Action: <Add/Modify>
VLAN ID:[1 ]          State:<Enabled >      Querier State:<Non-Querier>
Robustness Variable:[2 ] Query Interval:[125 ] Max Response:[10]  APPLY
-----

  VID   State   Age Out   Querier State
-----
  1     Enabled  260      Non-Querier

Age Out = Robustness Variable * Query Interval + Max Response
*****
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page

```

Figure 6-26. IGMP Snooping Settings screen

To configure IGMP Snooping:

Toggle the **Switch IGMP Snooping** field to *Enabled*. Toggle the **Querier State** field to the appropriate choice between *Non-Querier*, *V1-Querier*, and *V2-Querier* to determine the version of IGMP that is used in your network. A value between 1 and 255 can be entered for the **Robustness Variable** (default is 2). The **Query Interval** can be set between 1 and 65500 seconds (default is 125 seconds). This sets the time between IGMP queries. The **Max Response** allows a setting between 1 and 25 seconds (default is 10) and specifies the maximum amount of time allowed before sending a response report.

Highlight APPLY and press **Enter** to make the settings effective.

The user-changeable parameters in the switch are as follows:

- **Switch IGMP Snooping:**<Disabled> – This field can be toggled using the space bar between *Disabled* and *Enabled*. This is used to enable or disable IGMP Snooping, globally, on the switch.
- **Action:**<Add/Modify> – Toggle to the desired option, *Add/Modify* or *Delete*.
- **VLAN ID:**[1] – Enter the appropriate VLAN ID in this field.
- **State:**<Enabled> – Toggle this field to *Enabled* to activate this entry.
- **Querier State:**<Non-Querier> – This field can be toggled between *Non-Querier*, *V1-Querier*, and *V2-Querier*. This is used to specify the IGMP version (1 or 2) that will be used by the IGMP interface when making queries.
- **Robustness Variable:**[2] – A tuning variable to allow for sub-networks that are expected to lose a large number of packets. A value between 1 and 255 can be entered, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.
- **Query Interval:**[125] – Allows the entry of a value between 1 and 65500 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.

- **Max Response:[10]** – Sets the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered, with a default of 10 seconds.

Configure Trunk

To configure a port trunking group, highlight **Configure TRUNK** on the **Configuration** menu and press **Enter**.

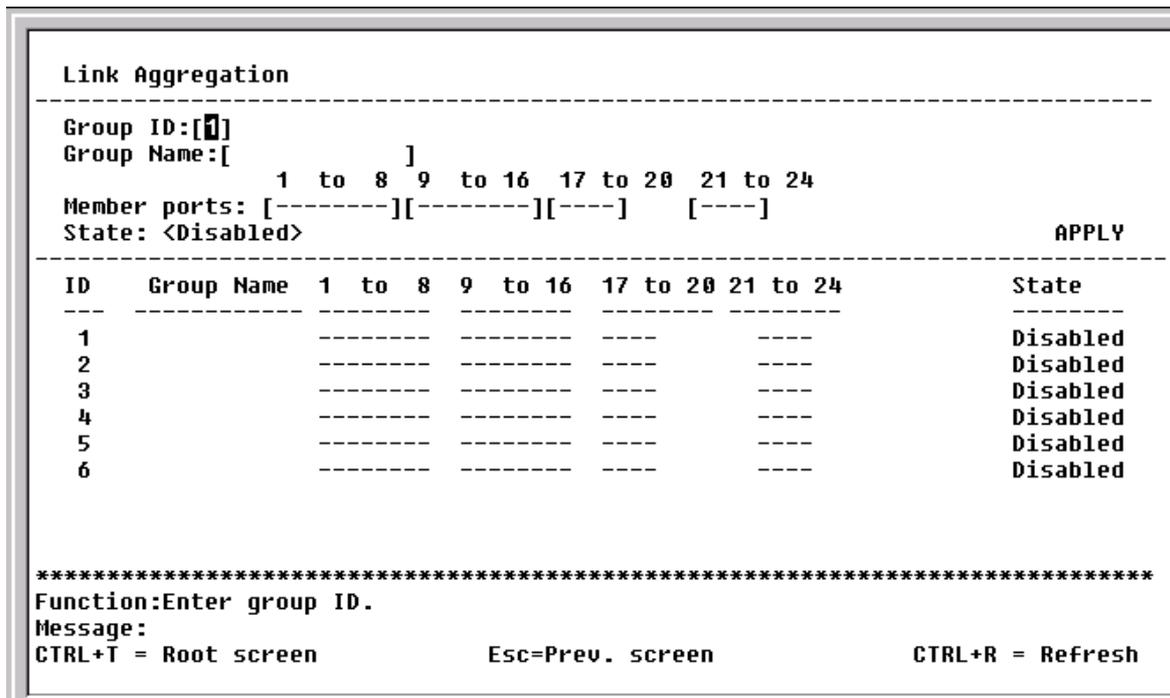


Figure 6-27. Link Aggregation screen

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

Port trunking is most commonly used to link a bandwidth intensive network device or devices – such as a server – to the backbone of a network.

The switch allows the creation of up to 6 port trunking groups, each group consisting of up to 16 links (ports). The trunked ports can be non-continuous (that is, have non-sequential port numbers). All of the ports in the group must be members of the same VLAN. Further, the trunked ports must all be of the same speed and should be configured as full duplex.

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

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

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

on the Switch, STP will block one entire group – in the same way STP will block a single port that has a redundant link.

The user-changeable parameters in the switch are as follows:

- **Group ID:**[1] – This field is for a group ID number for the port trunking group.
- **Group Name:**[] – Enter a name for the port trunking group.
- **Member ports** – Toggle between *M* to indicate membership of the port trunking group, or a dash (-) to indicate non-membership.
- **State:**<Disabled> – This field can be toggled between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.

Configure Port Mirroring

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

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

```

Setup Port Mirroring
-----

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

Source Port:<l  >
Source Direction:<Ingress & Egress>
Target Port:<ll  >
Mirror Status:<Disabled>

        APPLY

*****
Function:
Message:
CTRL+T = Root screen           Esc=Prev. screen           CTRL+R = Refresh

```

Figure 6-28. Setup Port Mirroring screen

To configure a mirror port, enter the port from where you want to copy frames in the **Source Port** field, select the desired source direction in the next field, and then enter the port that 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. Finally, toggle the **Mirror Status** field to *Enabled*, highlight **APPLY**, and press **Enter**.

Note: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port cannot be a member of a trunk group.

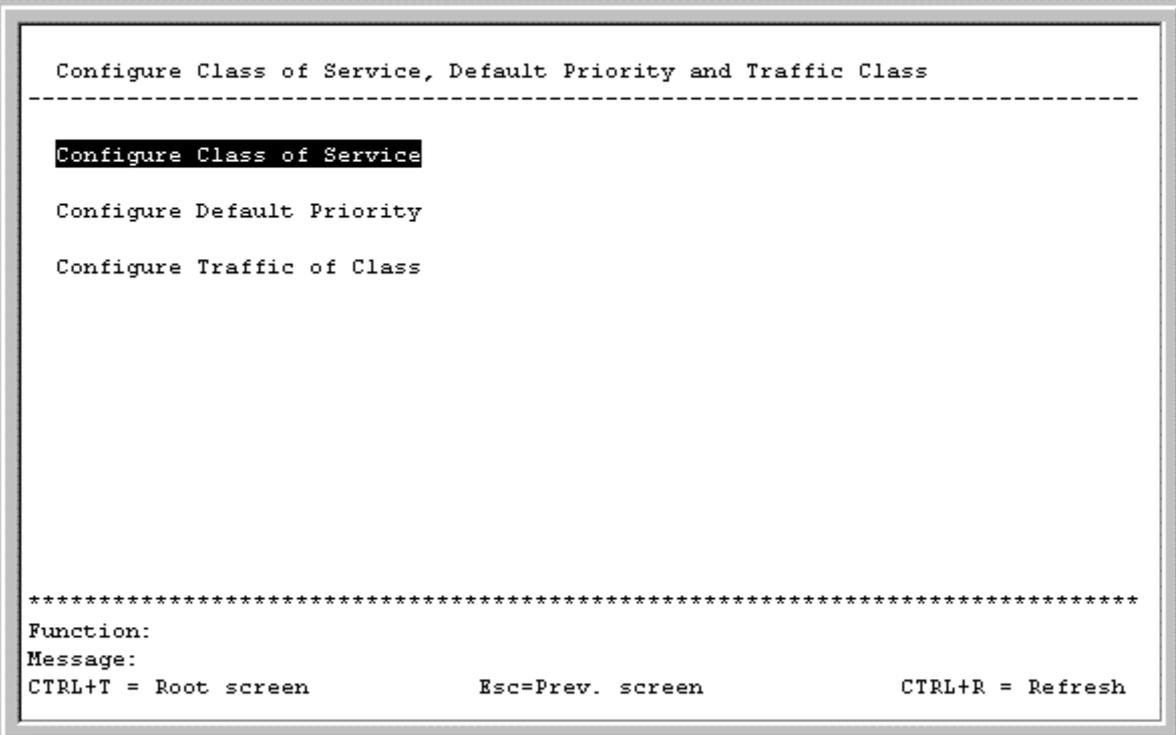
Note: Port mirroring is not possible if you use the same egress and ingress port.

Note: Port mirroring is only possible for ports 1–12 or ports 13–24. This means the source port and the target port must be between ports 1–12 or 13–24.

Configure Class of Service, Default Priority, and Traffic Class

The DGS-3224TG allows you to customize class of service, port default priority, and traffic class settings on the following menu.

Select **Configure Class of Service, Default Priority and Traffic Class** on the **Configuration** menu and press **Enter**.



```
Configure Class of Service, Default Priority and Traffic Class
-----
Configure Class of Service
Configure Default Priority
Configure Traffic of Class

*****
Function:
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh
```

Figure 6-29. Configure Class of Service, Default Priority and Traffic Class menu

Class of Service Configuration

Select **Configure Class of Service** and press **Enter** to access the following menu:

```

Class of Service Configuration
-----
                Max. Packets
                -----
Class-0 --> <No Limit >
Class-1 --> <No Limit >
Class-2 --> <No Limit >
Class-3 --> <No Limit >

                Max. Latency
                -----
                <3.2 se >

ADVANCED SETTINGS    APPLY

*****
Function:Input maximum packet count for a CoS Queue.(takes effect at roundRobin
mode)ge:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh

```

Figure 6-30. Class of Service Configuration menu

This menu allows you to set the following features:

- **Max. Packets** – Use the space bar in this column to select the maximum number of packets the Class of Service priority queue can hold. The range of values is from 0 to 512 packets.
- **Max. Latency** – The maximum allowable time a packet will stay in the CoS queue, in microseconds and seconds. The packets in this queue are not delayed more than the maximum allowable latency entered in this field. Maximum latency takes precedence over the CoS scheduling algorithm.

In addition, clicking **ADVANCED SETTINGS** at the bottom of the **Class of Service Configuration** menu will enable you to select the desired port queue priority:

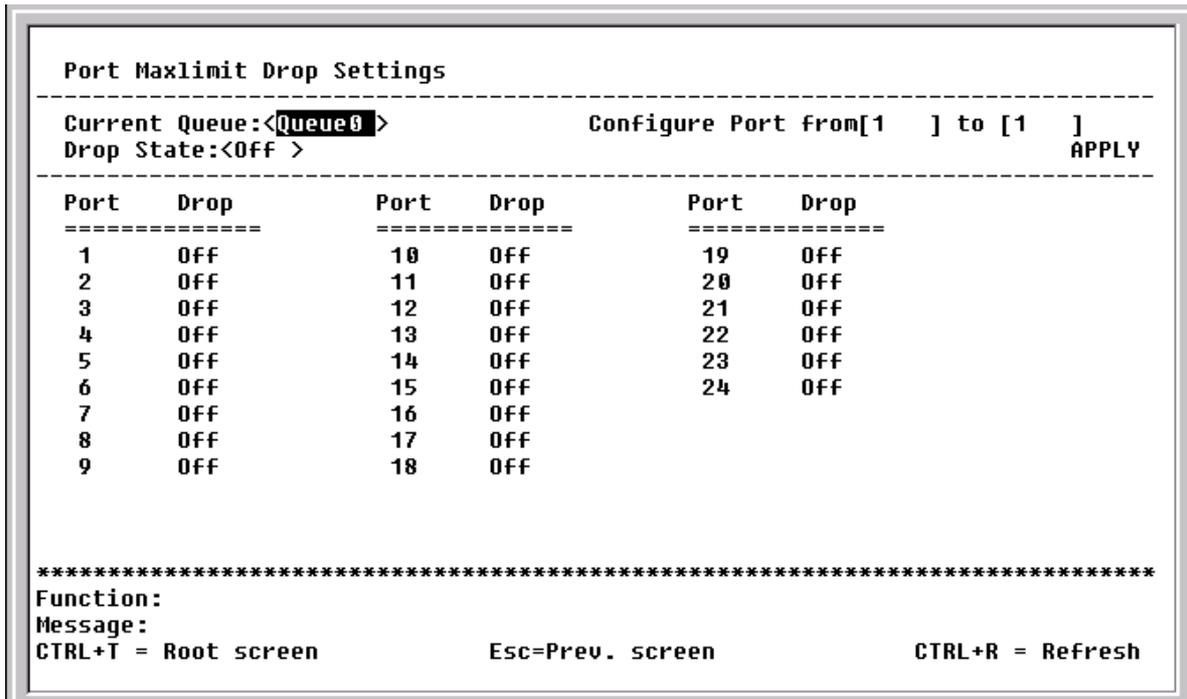


Figure 6-31. Port Maxlimit Drop Settings screen

The Switch divides the buffer into four parts: *Queue0*, *Queue1*, *Queue2*, and *Queue3*. *Queue0* is the highest priority and *Queue3* is the lowest. Press **APPLY** to let the change take effect.

Port Default Priority assignment

Select **Configure Default Priority** and press **Enter** to access the following screen:

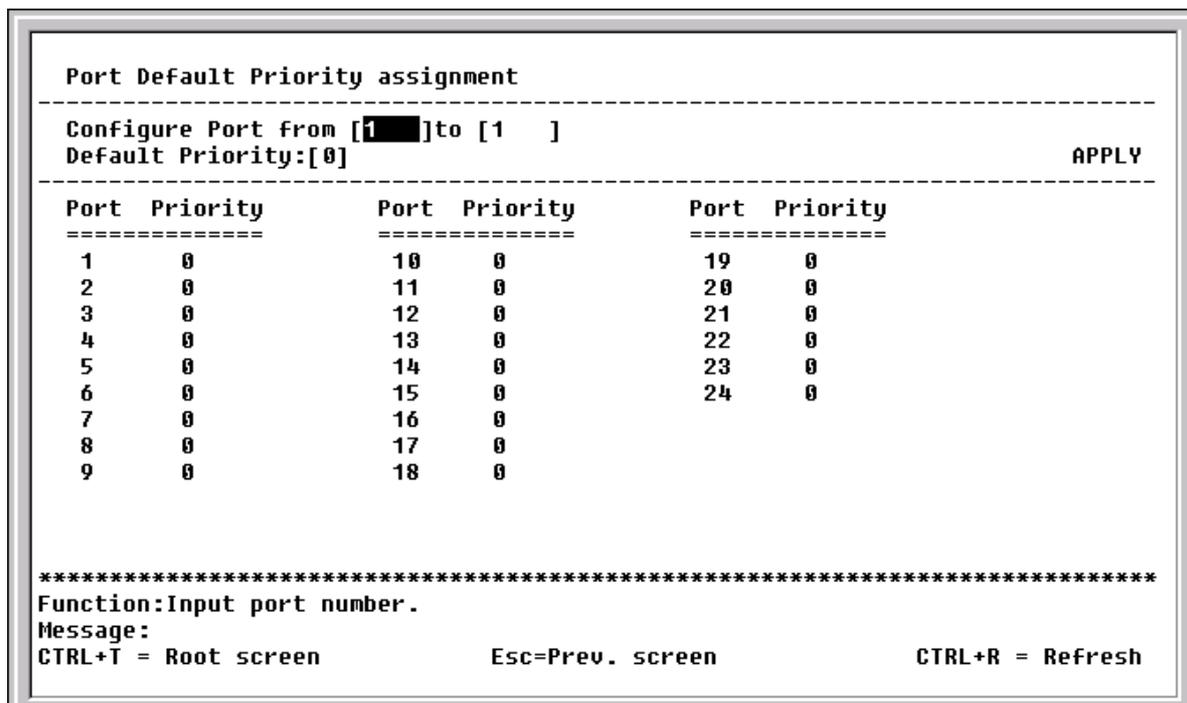


Figure 6-32. Port Default Priority assignment screen

This screen allows you to set a default priority for packets that have not already been assigned a priority value. After filling out the two fields offered, press APPLY to let your changes take effect.

Traffic Class Configuration

Select **Configure Traffic of Class** and press **Enter** to access the following screen:

```
Traffic Class Configuration
-----
Priority-0 --> <Class-0>
Priority-1 --> <Class-0>
Priority-2 --> <Class-1>
Priority-3 --> <Class-1>
Priority-4 --> <Class-2>
Priority-5 --> <Class-2>
Priority-6 --> <Class-3>
Priority-7 --> <Class-3>

      APPLY

*****
Function:Select the traffic class for this priority.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh
```

Figure 6-33. Traffic Class Configuration screen

This screen allows you to configure traffic class priority by specifying the class value, from 0 to 3, of the switch's eight levels of priority. Press APPLY to let your changes take effect.

Configure RS232 and SLIP

Select **Configure RS232 and SLIP** and press **Enter** to access the following screen:

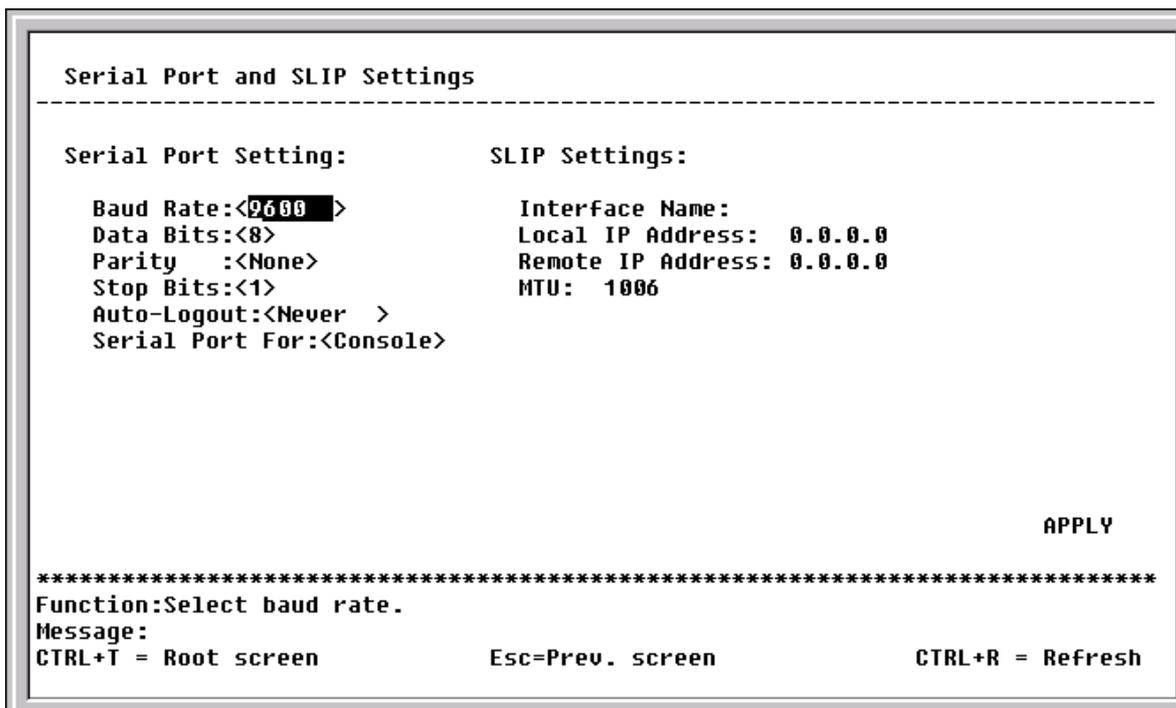


Figure 6-34. Serial Port and SLIP Settings screen

The following fields can then be set:

- **Baud Rate:**<9600> – Sets the serial bit rate that will be used to communicate the next time the switch is restarted. Available speeds are 9600, 19200, 38400 and 115200 bits per second. The default setting is 9600.
- **Data Bits:**<8> – Select 7 or 8. The default is 7.
- **Parity:**<None> – Choose from *None*, *Even* or *Odd*. The default is *None*.
- **Stop Bits:**<1> – Select 1 or 2. The default is 1.
- **Auto-Logout:**<Never> – This sets the time the interface can be idle before the switch automatically logs-out the user. The options are 2 mins, 5 mins, 10 mins, 15 mins, or *Never*.
- **Serial Port For:**<Console> – Change this field to *SLIP* and enter the appropriate information in the **Interface Name**, **Local IP Address**, **Remote IP Address**, and **MTU** fields which become active once *SLIP* is selected.

Network Monitoring

The DGS-3224TG provides extensive network monitoring capabilities.

To display the network data compiled by the switch, highlight **Network Monitoring** on the main menu and press **Enter**.

```

Network Monitoring Menu
-----
Port Utilization
Port Error Packets
Port Packet Analysis
Browse MAC Address
Switch History
IGMP Snooping
Browse Multicast Status
ULAN Status

*****
Function:Switch port utilization overview.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh

```

Figure 6-35. Network Monitoring Menu

Port Utilization

To view the port utilization of all the ports on the switch, highlight **Port Utilization** on the **Network Monitoring Menu** and press **Enter**:

```

Port Utilization
-----
                CLEAR COUNTER                Interval:< 2 sec >
Port    TX/sec    RX/sec    %Util.    Port    TX/sec    RX/sec    %Util.
-----
 1      0          46        1         14     0          0          0
 2      0          0          0         15     0          0          0
 3      0          0          0         16     0          0          0
 4      0          0          0         17     0          0          0
 5      0          0          0         18     0          0          0
 6      0          0          0         19     0          0          0
 7      0          0          0         20     0          0          0
 8      0          0          0         21     0          0          0
 9      0          0          0         22     0          0          0
10     0          0          0         23     0          0          0
11     0          0          0         24     0          0          0
12     0          0          0
13     0          0          0
*****
Function:Clear counter.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh

```

Figure 6-36. Port Utilization screen

The **Port Utilization** screen shows the number of packets transmitted and received per second and calculates the percentage of the total available bandwidth being used on the port (displayed under **%Util.**). Highlight **CLEAR COUNTER** and press **Enter** to reset the counters.

Port Error Packets

To view the error statistics for a port, highlight **Port Error Packets** on the **Network Monitoring Menu** and press **Enter**:

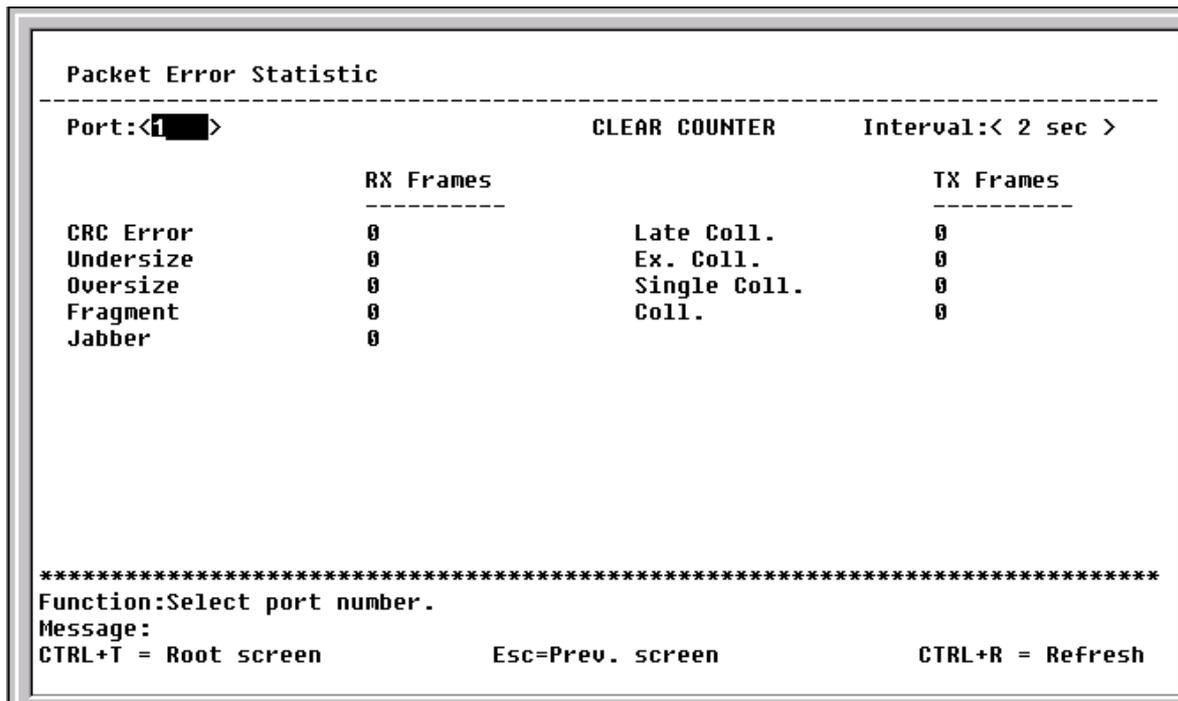


Figure 6-37. Packet Error Statistic screen

Enter the port number of the port to be viewed. The **Interval** field can be toggled from 2 seconds to 1 minute, or suspend. This sets the interval at which the error statistics are updated. Highlight **CLEAR COUNTER** and press **Enter** to reset the counters.

Port Packet Analysis

To view an analysis of the size of packets received or transmitted by a port, highlight **Port Packet Analysis** on the **Network Monitoring Menu** and press **Enter**:

```

Packet Analysis
-----
Port: <1 >
                                CLEAR COUNTER      Interval: < 2 sec >

      Frames  Frames/sec          Total      Total/sec
-----
64      5625      19          RX Bytes 3088391  4603
65-127   4939      4          RX Frames 14461    25
128-255  2066      0
256-511  695      0          TX Bytes  632     0
512-1023 175      0          TX Frames  8      0
1024-1518 969      2

Unicast RX  994      0
Multicast RX 2646    2
Broadcast RX 10821  23

*****
Function: Select port number.
Message:
CTRL+T = Root screen      Esc=Prev. screen      CTRL+R = Refresh

```

Figure 6-38. Packet Analysis screen

In addition to the size of packets received or transmitted by the selected port, statistics on the number of unicast, multicast, and broadcast packets are displayed. Highlight **CLEAR COUNTER** and press **Enter** to reset the counters.

Browse MAC Address

To view the MAC address forwarding table, highlight **Browse MAC Address** on the **Network Monitoring Menu** and press **Enter**:

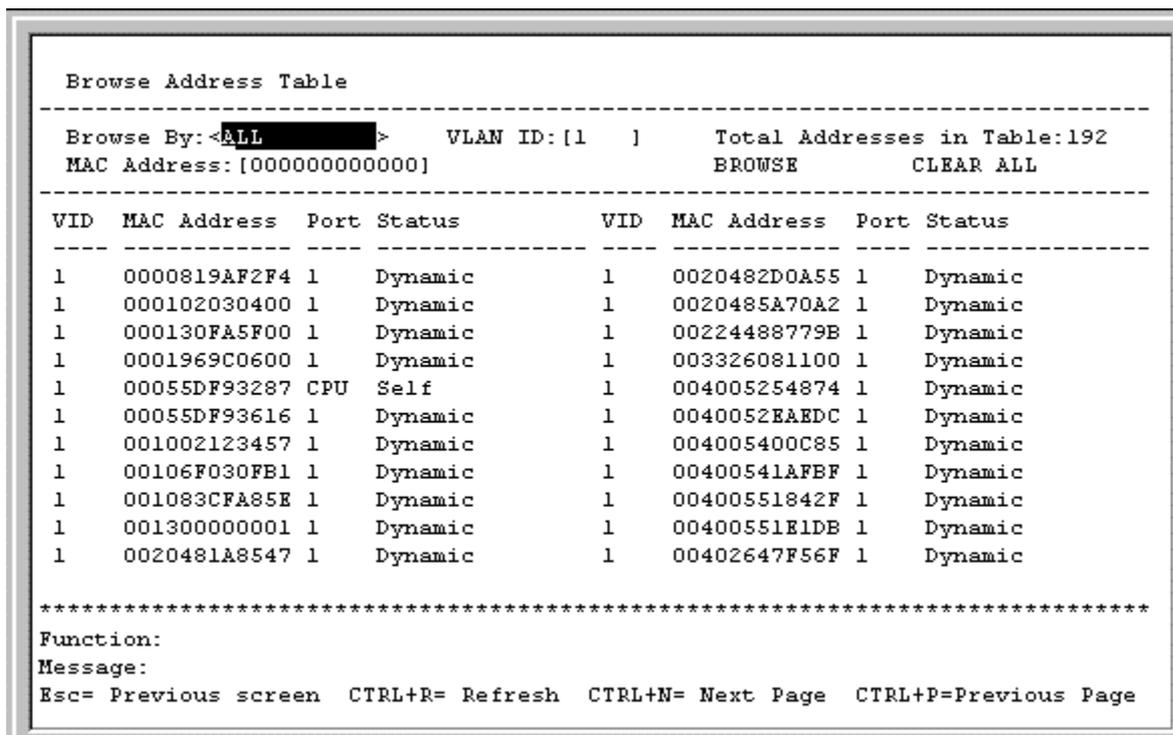


Figure 6-39. Browse Address Table screen

The **Browse By** field can be toggled between *ALL*, *MAC Address*, *Port*, and *VLAN*. This sets a filter to determine which MAC addresses from the forwarding table are displayed. *ALL* specifies no filter.

To search for a particular MAC address:

Toggle the **Browse By** field to **MAC Address**. A **MAC Address** field will appear. Enter the MAC address in the field and press **Enter**. Highlight **BROWSE** and press **Enter** to initiate the browsing action. Highlight **CLEAR ALL** and press **Enter** to reset the table counters.

Switch History

To view the switch history log, highlight **Switch History** from the **Network Monitoring Menu** and press **Enter**:

```

Switch History
-----
Seq. #      Time           Log Text
-----
155  2002/4/6 0:26:33  Successful login through console.
154  2002/4/5 23:58:38  Module 1, Port 1 Link Up
153  2002/4/5 23:58:35  Cold Start
152  2002/4/5 20:8:53   Upgrade firmware successfully.
151  2002/4/5 20:8:22   Module 1, Port 2 Link Up
150  2002/4/5 20:7:43   Successful login through console.
149  2002/4/5 20:7:40   Cold Start
148  2002/4/4 8:11:0    Configuration saved to flash.
147  2002/4/4 8:7:19   Configuration saved to flash.
146  2002/4/4 3:20:7   Successful login through console.
145  2002/4/4 3:16:31   Successful logout through console.
144  2002/4/4 2:46:25   Successful login through console.
- more (12 of 155)

*****
Function:View Switch Logs and Health Status
Message:
CTRL+N=Next Page CTRL+P=Previous Page B=Begin E=End C=Clear CTRL+R=Refresh

```

Figure 6-40. Switch History screen

IGMP Snooping

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

To view the IGMP Snooping table, highlight **IGMP Snooping** on the **Network Monitoring Menu** and press **Enter**.

```

IGMP Snooping Status
-----
VID:[1]          GO          Total Entries in the VLAN: 0
-----

VID: 1          State: Enabled  Age Out: 260      Queries:Non-Querier(0)
Multicast group:          1 to 8  9 to 16  17 to 20  21 to 24
MAC address:
Reports:

Multicast group:          1 to 8  9 to 16  17 to 20  21 to 24
MAC address:
Reports:

Multicast group:          1 to 8  9 to 16  17 to 20  21 to 24
MAC address:
Reports:
*****
Function:Enter VLAN ID
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
    
```

Figure 6-41. IGMP Snooping Status screen

Enter a VLAN ID number in the first field and press GO to display the desired **IGMP Snooping Status** screen.

Browse Multicast Status

```

Multicast Address Status
-----
VID  Group Addr.  Static/IGMP Snooping Port-list
-----

*****
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
    
```

Figure 6-42. Multicast Address Status screen

This read-only screen displays the VLAN ID, group address, and static/IGMP snooping port list for multicast addresses.

VLAN Status

This allows the status for each of the switch's VLANs to be viewed.

To view the **VLAN Status** table, highlight **VLAN Status** on the **Network Monitoring Menu** and press **Enter**.

```

- VLAN Status
-----
Number of IEEE 802.1Q VLAN: 1

IEEE 802.1Q VLAN ID: 1

Current Egress Ports:  1,  2,  3,  4,  5,  6,  7,  8,  9, 10,
                      11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
                      21, 22, 23, 24, CPU
Current Untagged Ports 1,  2,  3,  4,  5,  6,  7,  8,  9, 10,
                      11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
                      21, 22, 23, 24

Status: Permanent

Creation time since switch power up: 10:30:02

*****
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page

```

Figure 6-43. VLAN Status screen

This read-only screen displays VLAN information. Press CTRL + N to see the VLAN on the next page or CTRL + P to see an entry from a previous page.

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 and Operating Concepts.”

SNMP (V1) 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** to access the third item on the main menu. The following screen appears:

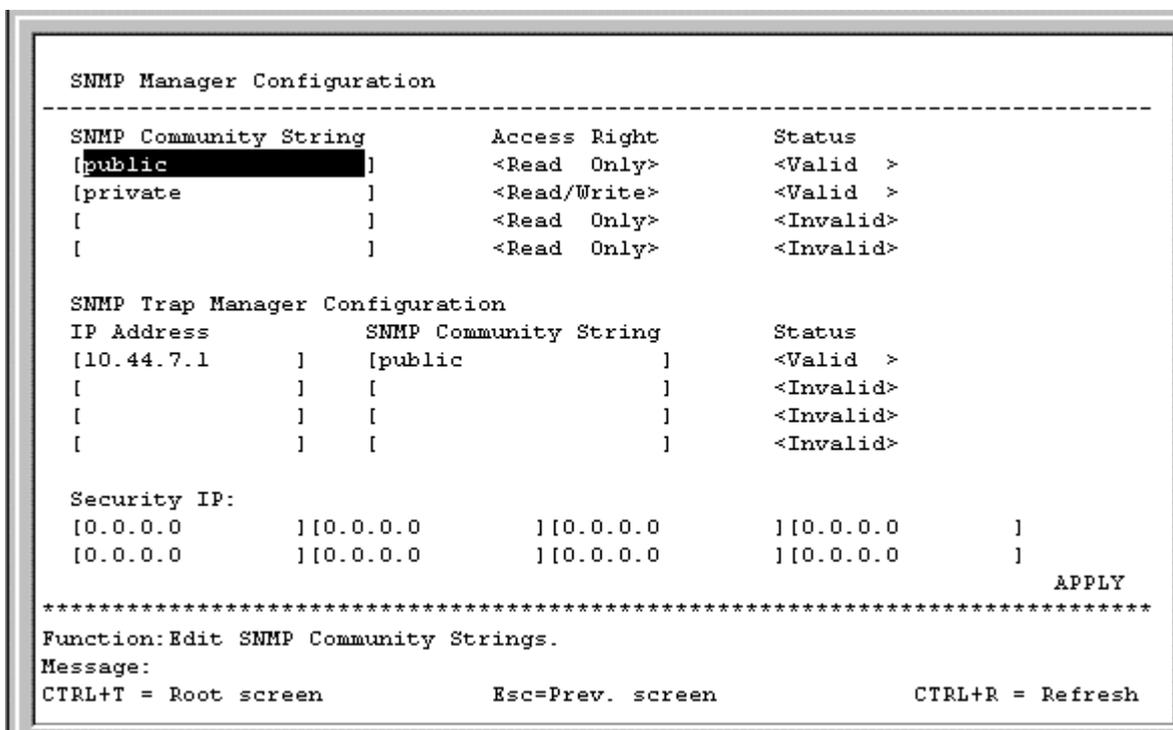


Figure 6-44. SNMP Manager Configuration screen

The following SNMP Manager and Trap Manager Configuration parameters can be set:

- **SNMP Community String** – The community string that will be included on SNMP packets sent to and from the switch. Any station not privy to this community will not receive the packet.
- **Access Right** – Allows each community to be separately set to either *Read Only*, meaning that the community member can only view switch settings or *Read/Write*, which allows the member to change settings in the switch.
- **Status** – Determines whether this community name entry is *Valid* or *Invalid*. An entry can be disabled by changing its status to *Invalid*.
- **IP Address** – The IP address of the network management station to receive traps.

The Security IP section allows you to create a list of IP addresses that are allowed to access the switch via SNMP or Telnet.

Highlight **APPLY** and press **Enter** to allow your changes to take effect.

System Utilities

To access the **Switch Utilities** menu, highlight **System Utilities** on the main menu and press **Enter**.

```
Switch Utilities
-----

Switch Settings:

Server IP Address: 10.43.10.1
Switch IP Address: 10.24.22.3
Subnet Mask: 255.0.0.0
Gateway Router: 10.254.254.251

TFTP Services:                Others:

Upgrade Firmware from TFTP Server  Ping Test
Use Configuration File on TFTP Server
Save Settings to TFTP Server
Save History Log to TFTP Server

*****
Function: Upgrade firmware from TFTP server.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh
```

Figure 6-45. Switch Utilities menu

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

Upgrade Firmware from TFTP Server

To update the switch's firmware, highlight **Upgrade Firmware from TFTP Server** and press **Enter**.

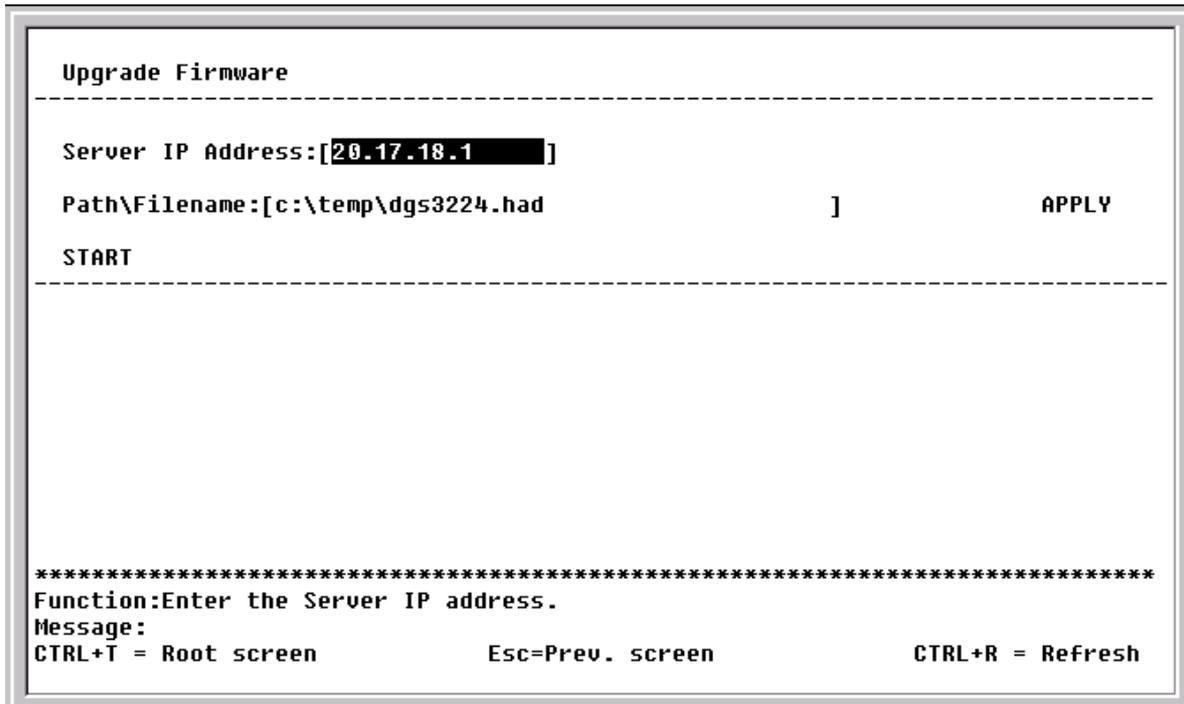


Figure 6-46. Upgrade Firmware screen

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

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

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

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

Highlight APPLY and press **Enter** to record the IP address of the TFTP server. Use **Save Changes** from the main menu to enter the address into NV-RAM

Highlight START and press **Enter** to initiate the file transfer.

Use Configuration File on TFTP Server

To download a switch configuration file from a TFTP server, highlight **Use a Configuration File on TFTP Server** and press **Enter**.

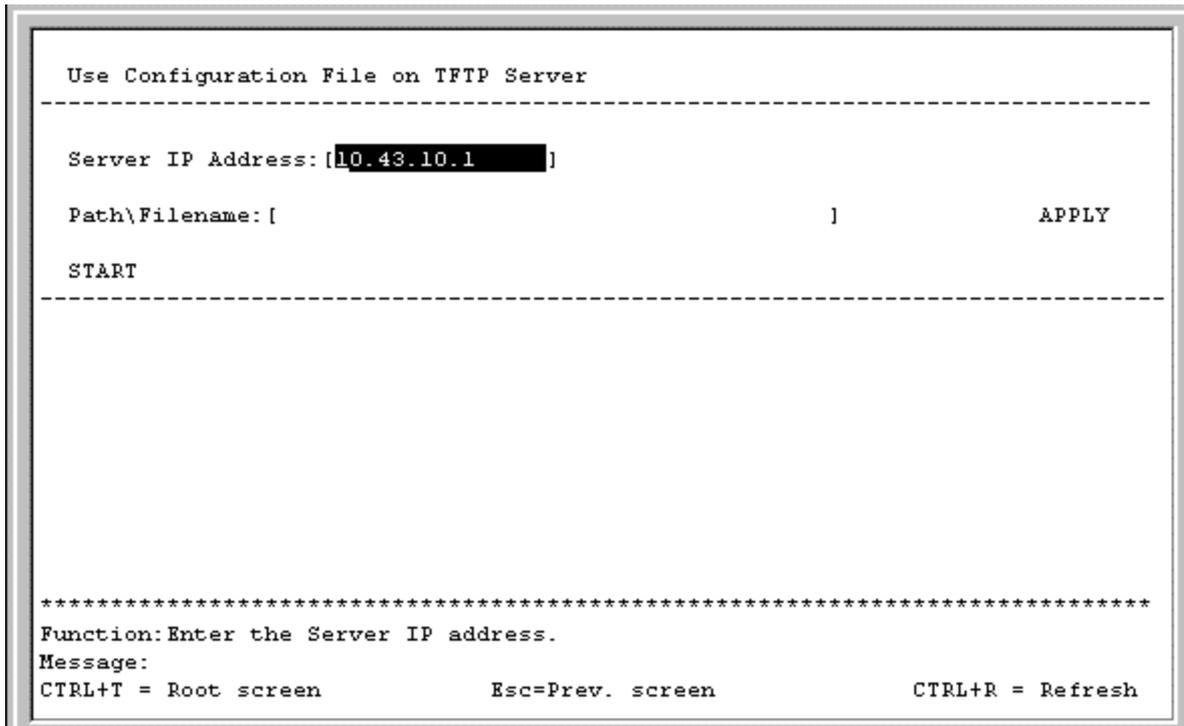


Figure 6-47. Use Configuration File on TFTP Server screen

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

Highlight **APPLY** and press **Enter** to record the IP address of the TFTP server. Use **Save Changes** from the main menu to enter the address into NV-RAM

Highlight **START** and press **Enter** to initiate the file transfer.

Save Settings to TFTP Server

To upload a settings file to the TFTP server, highlight **Save Settings to TFTP Server** and press **Enter**.

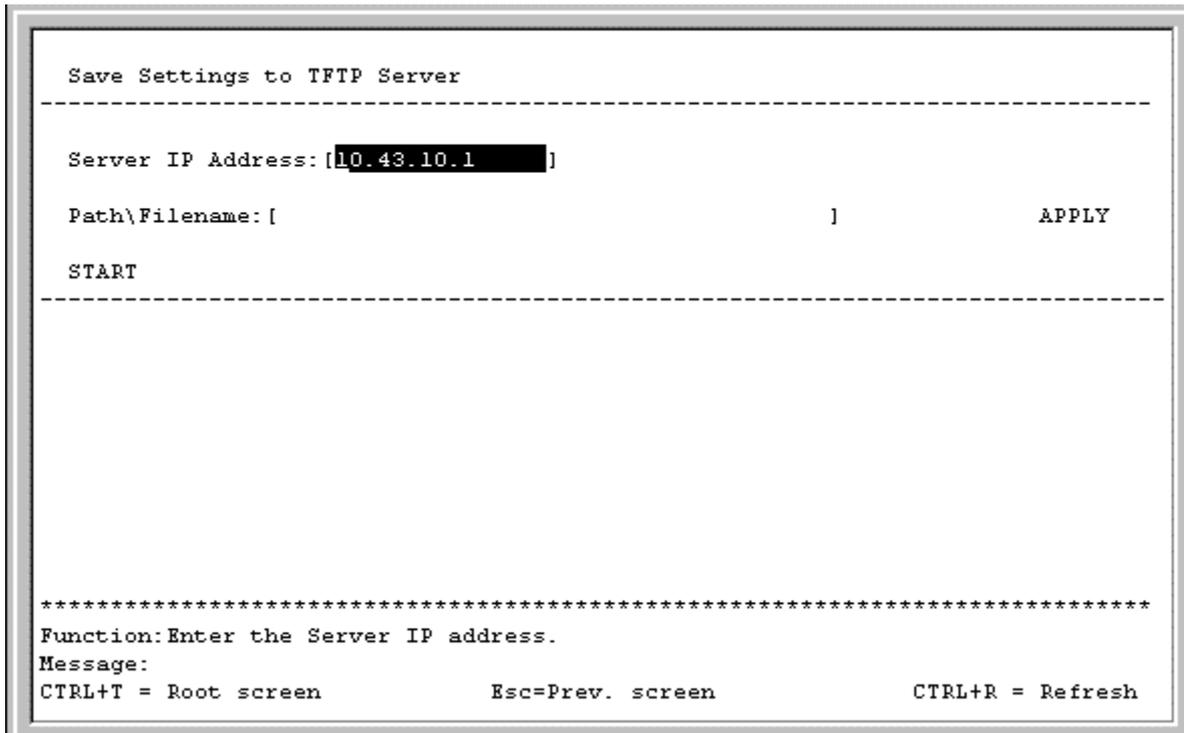


Figure 6-48. Save Settings to TFTP Server screen

Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server and press APPLY. Highlight START and press **Enter** to initiate the file transfer.

Save History Log to TFTP Server

To save a History Log on a TFTP server, highlight **Save History Log to TFTP Server** and press **Enter**.

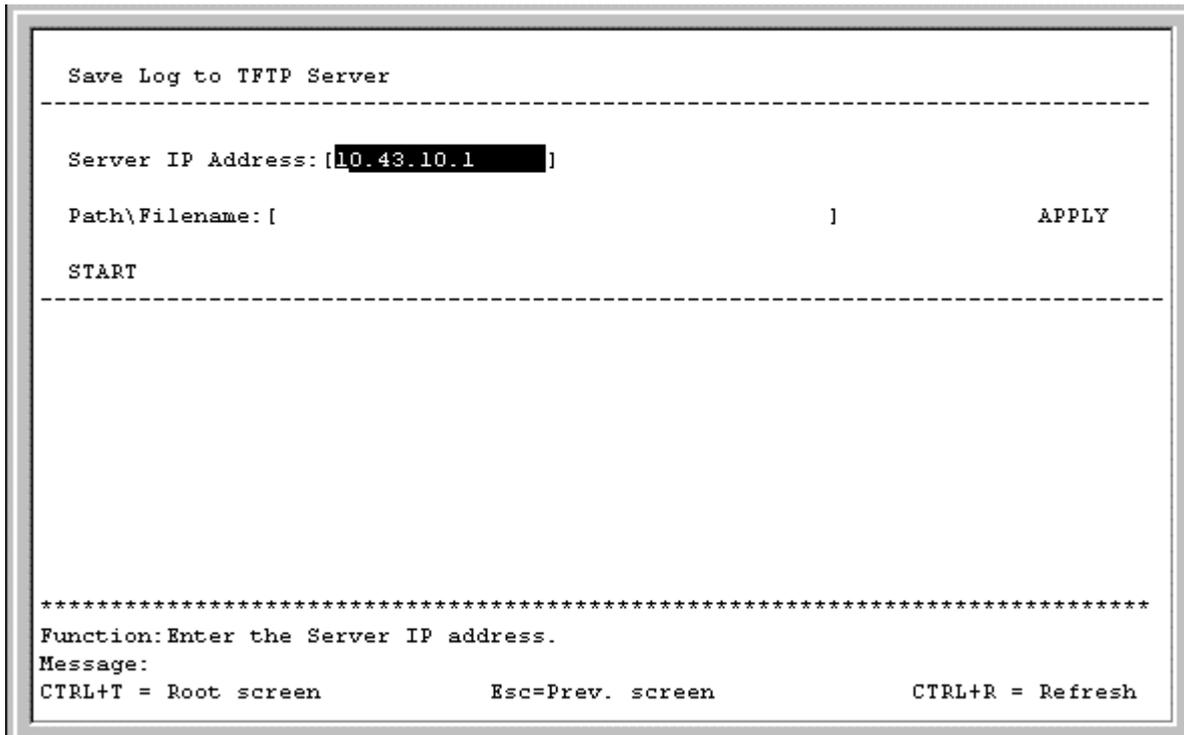


Figure 6-49. Save Log to TFTP Server screen

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. Highlight **APPLY** and press **Enter** to make the changes current. Highlight **START** and press **Enter** to initiate the file transfer.

Ping Test

To test the connection with another network device using Ping, highlight **Ping Test** and press **Enter**.

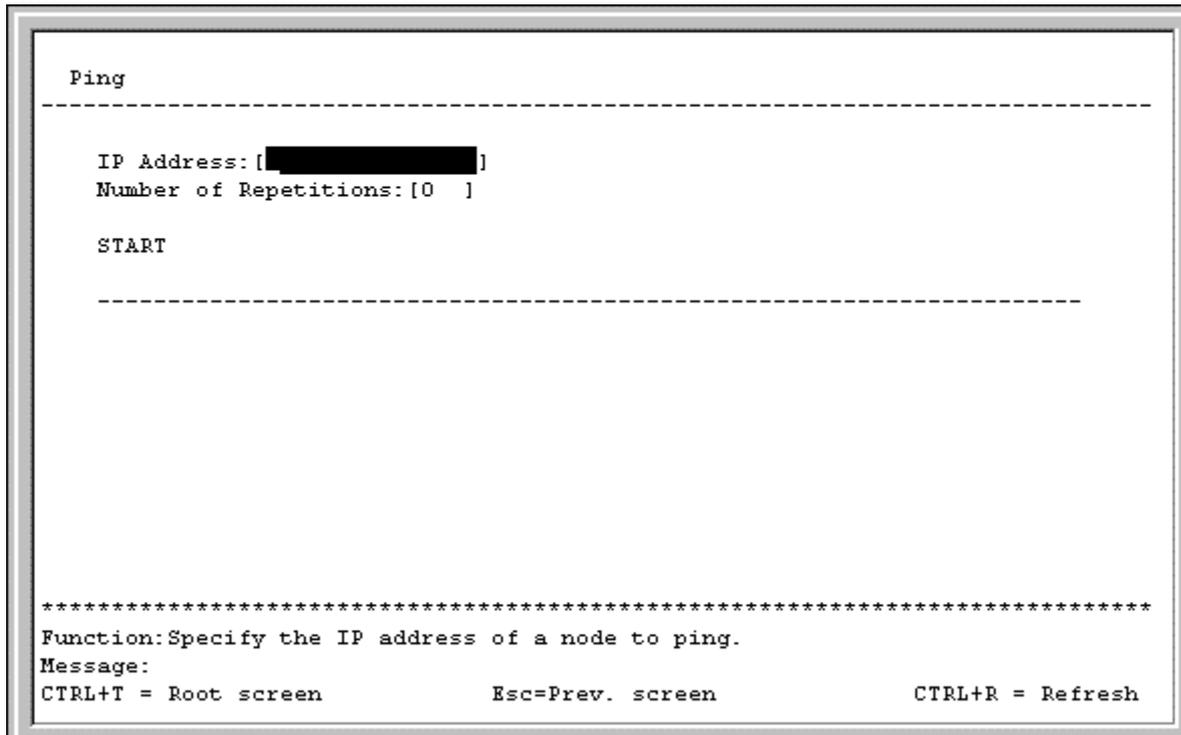


Figure 6-50. Ping screen

Enter the IP address of the network device to be Pinged and the number of test packets to be sent (3 is usually enough). Highlight **START** and press **Enter** to initiate the Ping program.

Reboot

The DGS-3224TG has several reboot options.

To reboot the switch from the console, highlight **Reboot** from the main menu and press **Enter**.

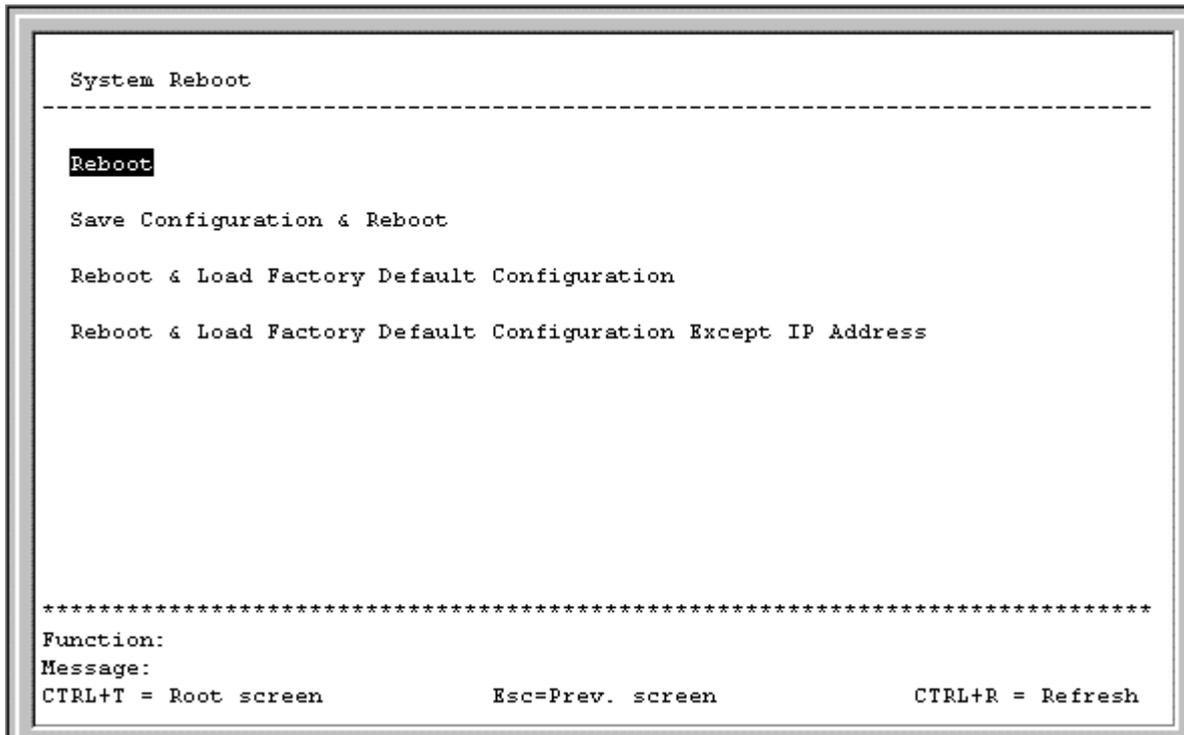


Figure 6-51. System Reboot menu

The reboot options are as follows:

- **Reboot** – Simply restarts the switch. Any configuration settings not saved using **Save Changes** from the main menu will be lost. The switch's configuration will be restored to the last configuration saved in NV-RAM.
- **Save Configuration & Reboot** – Saves the configuration to NV-RAM (identical to using **Save Changes**) and then restarts the switch.
- **Reboot & Load Factory Default Configuration** – Restarts the switch using the default factory configuration. All configuration data will be lost. This is identical to using **Factory Reset** and then **Reboot**.
- **Reboot & Load Factory Default Configuration Except IP Address** – Restarts the switch using the default factory configuration, except the user configured IP address will be retained. All other configuration data will be lost.

A confirmation screen will appear:

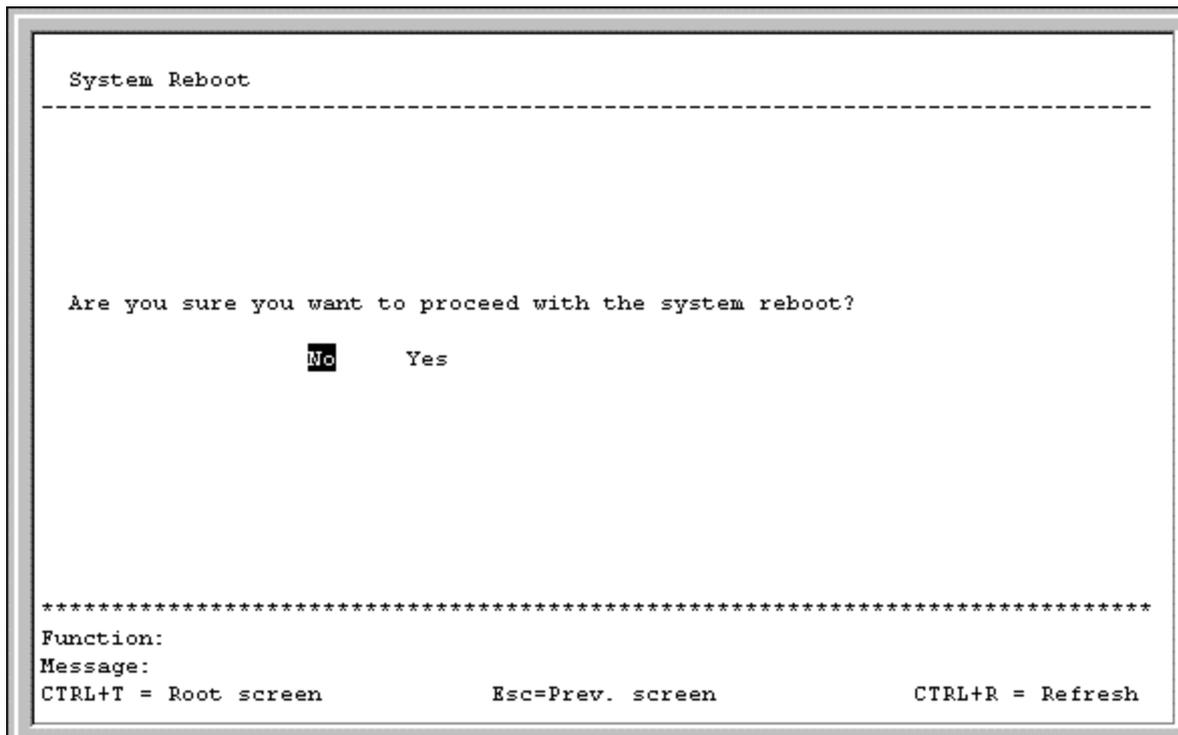


Figure 6-52. System Reboot confirmation screen

To reboot the switch, in the mode entered above, highlight Yes and press **Enter**.

WEB-BASED NETWORK MANAGEMENT

Introduction

The DGS-3224TG offers an embedded Web-based (HTML) interface allowing users to manage the switch from anywhere on the network through a standard browser, such as Opera, Netscape Navigator/Communicator, or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the switch using the HTTP protocol. Your browser window may vary with the screen shots (pictures) in this guide.

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

Note: This Web-based Management Module does not accept Chinese language input (or other languages requiring 2 bytes per character).

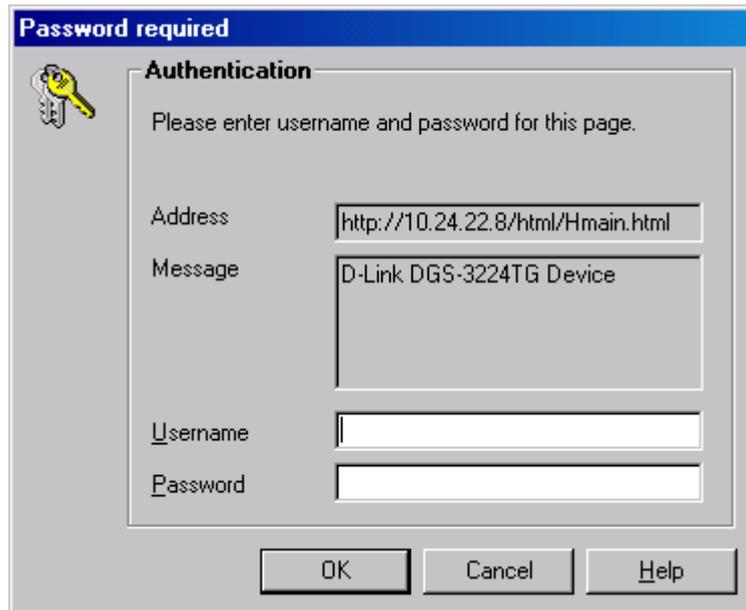
Getting Started

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 that allows a person to read hypertext, for example, Opera, 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 should be done manually through a console (see the *Configure IP Address* section in the “Using The Console Interface” chapter).

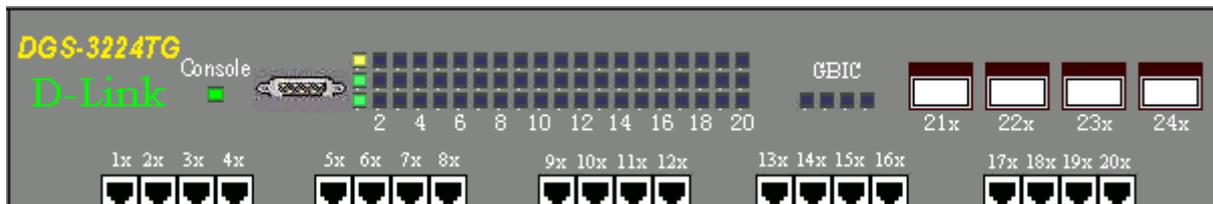
You are now ready to begin managing your switch by simply running the browser installed on your computer and pointing it to the IP address you have defined for the device. The URL in the address bar should read something like: `http://123.123.123.123`, where the numbers 123 represent the IP address of the switch. Please note that the proxy for session connection should be turned off.

Depending on which browser you are using, a dialog box similar to the following will open:

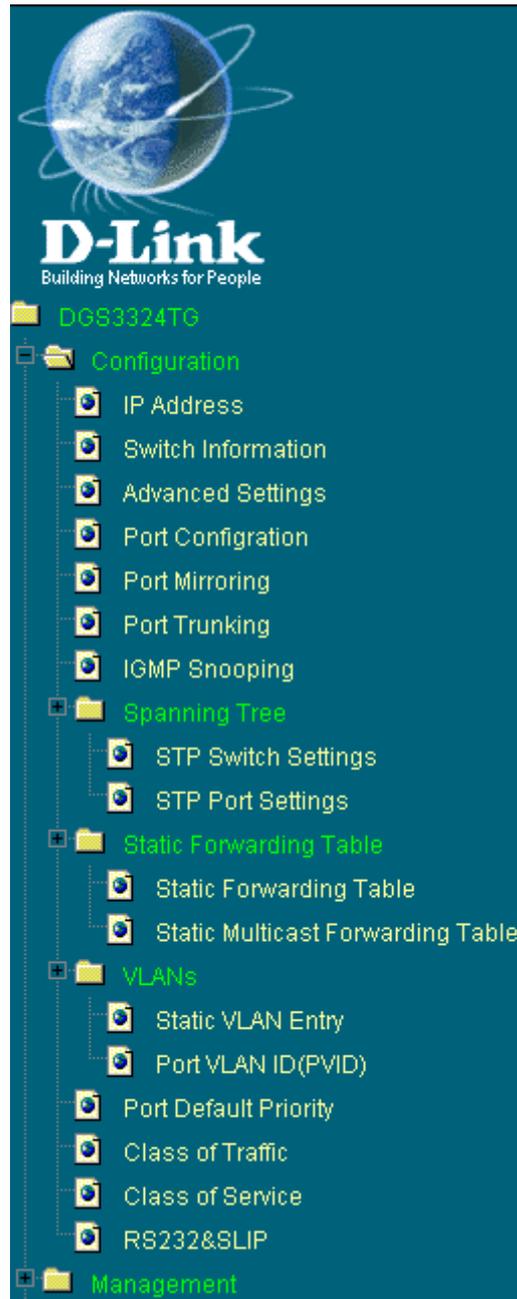


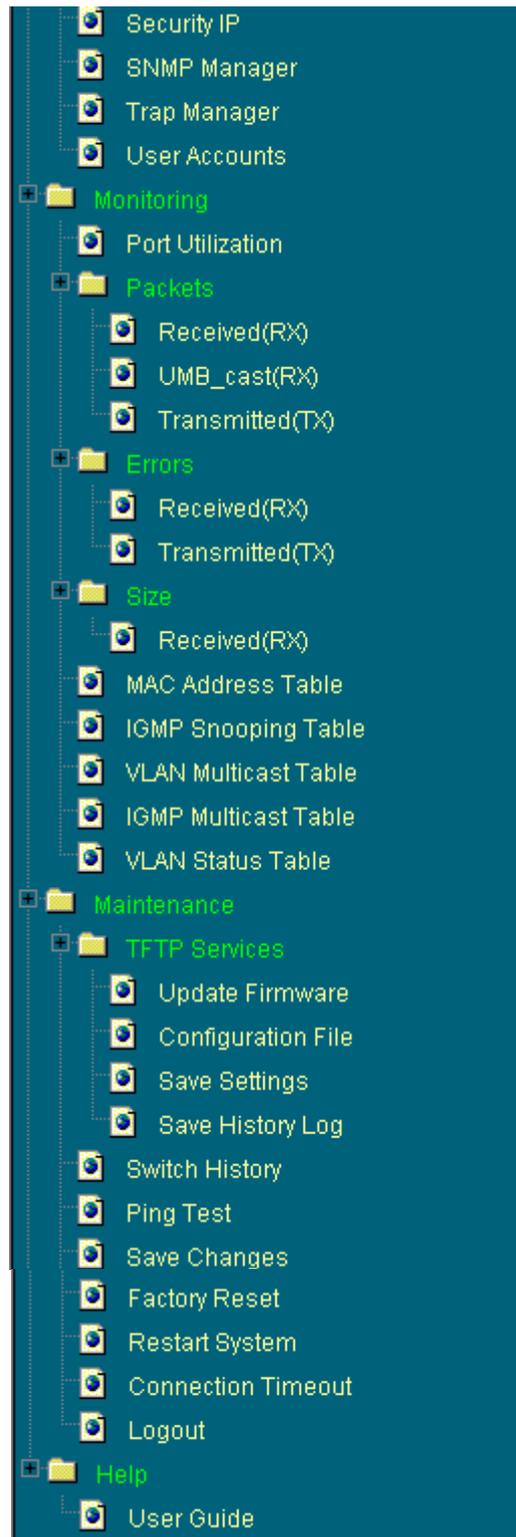
Click **OK** as there is no preset user name or password on the switch. This opens the main page in the management module.

The top panel shows a real-time front panel display of the DGS-3224TG. Clicking on an individual port on this display will connect you to the **Rx Packets Analysis** window (see **Monitoring**→**Packets**→**Received(RX)**) for a detailed description)



The panel on the left-hand side contains the main menu. The featured items include: **Configuration**, **Management**, **Monitoring**, **Maintenance**, and **Help**. The whole menu looks like this:





These are the major categories for switch management. If the sub-menus for each main category do not appear, click on the small square hyperlink to the left of the folder icon.

The switch management features available in the Web-based are explained below.

Configuration

The first category includes: **IP Address**, **Switch Information**, **Advanced Settings**, **Port Configuration**, **Port Mirroring**, **Port Trunking**, **IGMP Snooping**, **Spanning Tree**, **Static Forwarding Table**, **VLANs**, **Port Default Priority**, **Class of Traffic**, **Class of Service**, and **RS232&SLIP**, as well secondary screens.

IP Address

TCP/IP Parameters Setup	
MAC Address	00:05:5d:f9:32:87
Get IP From	Manual
IP Address	10.24.22.8
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
VID	1

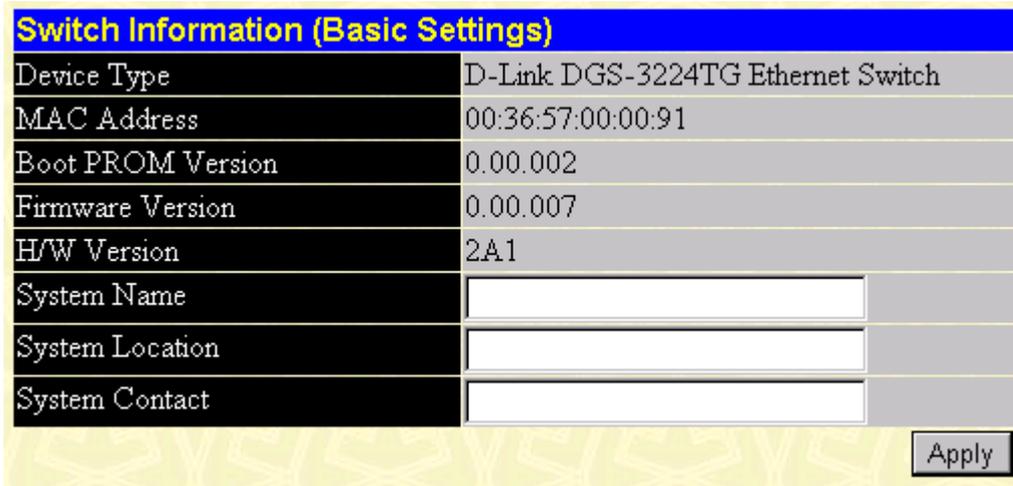
Figure 7-1. TCP/IP Parameters Setup window

This window is used to determine whether the switch should get its IP Address settings from the user (*Manual*), a *BOOTP* server, or a *DHCP* server. If you are not using either *BOOTP* or *DHCP*, 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. If you enable *DHCP*, a Dynamic Host Configuration Protocol request will be sent when the switch is powered up. Once you have selected a setting under **Get IP From**, click **Apply** to activate the new settings.

The information is described as follows:

- **MAC Address** – The Ethernet address for the device. Also known as the physical address
- **Get IP From** – There are three choices for how the switch receives its IP Address settings: *Manual*, *BOOTP*, and *DHCP*.
- **IP Address** – The host address for the device on the TCP/IP network.
- **Subnet Mask** – The address mask that controls subnetting on your TCP/IP network.
- **Default Gateway** – The IP address of the device, usually a router, that handles connections to other subnets and/or other TCP/IP networks.
- **VID** – The VLAN ID number.

Switch Information



Switch Information (Basic Settings)	
Device Type	D-Link DGS-3224TG Ethernet Switch
MAC Address	00:36:57:00:00:91
Boot PROM Version	0.00.002
Firmware Version	0.00.007
H/W Version	2A1
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>

Apply

Figure 7-2. Switch Information (Basic Settings) window

To set basic switch settings, enter a **System Name** in the first field, the physical location of the switch in the **System Location** field, and the name of the contact person responsible for the switch in the **System Contact** field. Then click **Apply**.

The information is described as follows:

- **Device Type** – A description of the switch type.
- **MAC Address** – The Ethernet address for the device.
- **Boot PROM Version** – Version number for the firmware chip. This information is needed for new runtime software downloads.
- **Firmware Version** – Version number of the firmware installed on the switch. This can be updated by using the **Update Firmware** window in the **Reset and Update** section.
- **H/W Version** – Version of the switch hardware.
- **System Name** – A user-assigned name for the switch.
- **System Location** – A user-assigned description for the physical location of the switch.
- **System Contact** – Name of the person to contact should there be any problems or questions with the system. You may also want to include a phone number or extension.

Advanced Settings

Switch Information (Advanced Settings)			
Auto Logout	Never		
MAC Address Aging Time [10-2100(sec)]	300		
IGMP Snooping	Disabled		
GVRP Status	Enabled		
Scheduling Mechanism for CoS Queues	Strict		
Trunk Load Sharing Algorithm	Source Addr		
Year/Month/Date	2002	4	4
Hour/Minute/Second	8	32	34
Apply			

Figure 7-3. Switch Information (Advanced Settings) window

After making the desired advanced setting Layer 2 changes, click **Apply** to let them take effect.

The information in the window is described as follows:

- **Auto-Logout** [*Never*] – This sets the time the interface can be idle before the switch automatically logs-out the user. The options are *2 minutes*, *5 minutes*, *10 minutes*, *15 minutes*, or *Never*.
- **MAC Address Aging Time [10-2100(sec)]** [*300*] – This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between 10 and 2100 seconds.

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

- **IGMP Snooping** [*Disabled*] – This setting enables Internet Group Management Protocol (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).
- **GVRP Status** [*Enabled*] – Group VLAN Registration Protocol is a protocol that allows members to dynamically join VLANs. This is used to enable or disable GVRP on the switch
- **Scheduling Mechanism for CoS Queues** [*Strict*] – There are two Class of Service queue options, *RoundRobin* and *Strict*. If *Strict* is selected, when the highest priority queue is full, those packets will be the first to be forwarded. If *RoundRobin* is selected, the forwarding is based on the settings made on the **Class of Service Configuration** screen.
- **Trunk Load Sharing Algorithm** [*Source Addr*] – The trunk load sharing options are *Destination Addr*, *Src & Dest Addr*, and *Source Addr*.
- **Year/Month/Date** – This allows you to set the year, month, and date.
- **Hour/Minute/Second** – This allows you to set the hour, minute, and second.

Port Configuration

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

The Port Information Table					
Port	State	Speed/Duplex	Flow Control	Connection	Port Type
1	Enabled	AUTO	AUTO	100M/Full/None	1000TX
2	Enabled	AUTO	AUTO	-	1000TX
3	Enabled	AUTO	AUTO	-	1000TX
4	Enabled	AUTO	AUTO	-	1000TX
5	Enabled	AUTO	AUTO	-	1000TX
6	Enabled	AUTO	AUTO	-	1000TX
7	Enabled	AUTO	AUTO	-	1000TX
8	Enabled	AUTO	AUTO	-	1000TX
9	Enabled	AUTO	AUTO	-	1000TX
10	Enabled	AUTO	AUTO	-	1000TX
11	Enabled	AUTO	AUTO	-	1000TX
12	Enabled	AUTO	AUTO	-	1000TX
13	Enabled	AUTO	AUTO	-	1000TX
14	Enabled	AUTO	AUTO	-	1000TX
15	Enabled	AUTO	AUTO	-	1000TX
16	Enabled	AUTO	AUTO	-	1000TX
17	Enabled	AUTO	AUTO	-	1000TX
18	Enabled	AUTO	AUTO	-	1000TX
19	Enabled	AUTO	AUTO	-	1000TX
20	Enabled	AUTO	AUTO	-	1000TX
21	Enabled	1000M/FULL	Enabled	-	None
22	Enabled	1000M/FULL	Enabled	-	None
23	Enabled	1000M/FULL	Enabled	-	None
24	Enabled	1000M/FULL	Enabled	-	None

Figure 7-4. Port Configuration window

Select the port you want to configure by using the drop-down menus in the **From** and **To** fields. Follow these steps:

1. Enable or disable the port. If you choose *Disabled* in the **State** field, 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.
2. Configure the **Speed/Duplex** setting for the twenty 10/100/1000 ports. Select *Auto* to allow the port to select the best transmission speed, duplex mode, and flow control settings based on the

capabilities of the device at the other end. The other selections allow you to force the port to operate in the specified manner. Select *1000M/Full* for port operation at 1000 Mbps and full duplex. Select *100M/Half* for port operation at 100 Mbps and half duplex. Select *100M/Full* for port operation at 100 Mbps and full duplex. Select *10M/Half* for port operation at 10 Mbps and half duplex. Select *10M/Full* for port operation at 10 Mbps and full duplex. The four GBIC ports are *1000M/Full* only.

- Configure the **Flow Control** setting for the port. Selecting *Enabled* in full-duplex mode will implement IEEE 802.3x flow control. Select *Disabled* for no flow control. Also, if the port is set for *Auto* (NWay) in the speed/duplex field above and flow control is enabled, flow control (whether full- or half-duplex) will only be implemented if the other device can auto-negotiate flow control.
- Click **Apply** to let your changes take effect.

Port Mirroring

Port Mirroring	
Source Port	Port 1
Source Direction	None
Ingress Target Port	Port 11
Egress Target Port	Port 11

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

Note(2): The target port should be a non-trunked port.

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, first select the **Source Port**—from where you want to copy frames—and the **Ingress Target Port** or **Egress Target 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. Next, select the **Source Direction**, *Ingress*, *Egress*, or *Ingress & Egress*, and *None* from the **Status** pull-down menu. Finally, click **Apply** to let the changes take effect.

Note: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

Port Trunking

Port Trunking Settings

ID	Name	Member Ports																								State	Active
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		
1	<input type="text"/>	<input type="checkbox"/>	Disabled	Apply																							
2	<input type="text"/>	<input type="checkbox"/>	Disabled	Apply																							
3	<input type="text"/>	<input type="checkbox"/>	Disabled	Apply																							
4	<input type="text"/>	<input type="checkbox"/>	Disabled	Apply																							
5	<input type="text"/>	<input type="checkbox"/>	Disabled	Apply																							
6	<input type="text"/>	<input type="checkbox"/>	Disabled	Apply																							

Note: It is only valid to set up at most 16 member ports of any one trunk group and a port can be a member of only one trunk group at a time.

Figure 7-6. Port Trunking Settings window

The Switch supports up to 6 trunk groups. Trunks are groups of ports that are banded together to form a single, logical, high-bandwidth data pipe. The maximum number of member ports for a trunk group is 16.

To create or modify a trunk group, enter a name in the first field, check the ports that will compose the port trunk, and change the **Status** field to *Enabled*. Click **Apply** to activate your settings.

Items in the above window are defined as follows:

- **Name** – The user-assigned name of the trunk group.
- **Member Ports** – Check the number of ports that will be members of the trunk group.
- **State** – Enables or disables the trunk group.

IGMP Snooping

IGMP Snooping Settings

VLAN ID	State	Querier State	Robustness Variable	Query Interval	Max Response	Add/Modify
1	Disabled	Non-Querier	2	125	10	Apply

IGMP Snooping Setup Table Entries: 1

VID	State	Robustness Variable	Query Interval	Max Response	Age Out	Querier State	Delete
1	Enabled	2	125	10	260	Non-Querier	<input type="checkbox"/>

End of data!

Figure 7-7. IGMP Snooping Settings window

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

To set up IGMP snooping, enter a VLAN ID number in the first field and change the **State** field to *Enabled*. Next, select the desired setting in the **Querier State** field—this determines the version of IGMP that is used in your network—and enter values in the following three fields. A value between 1 and 255 can be entered for the **Robustness Variable** (default is 2). The **Query Interval** can be set between 1 and 65500 seconds. This sets the time between IGMP queries. The **Max Response** allows a setting between 1 and 25 seconds and specifies the maximum amount of time allowed before sending a response report. Click **APPLY** to make the settings effective.

The user-changeable parameters in the switch are as follows:

- **VLAN ID/VID** – Enter a VLAN ID number in this field.
- **State** – Use the drop-down menu to enable or disable IGMP settings.
- **Querier State** – Select from *Non-Querier*, *V1-Querier*, and *V2-Querier*. This is used to specify the IGMP version (1 or 2) that will be used by the IGMP interface when making queries.
- **Robustness Variable** – A tuning variable to allow for sub-networks that are expected to lose a large number of packets. A value between 1 and 255 can be entered, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.
- **Query Interval** – Allows the entry of a value between 1 and 65500 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
- **Max Response** – Sets the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered.
- **Add/Modify** – Click this hyperlink to add or modify an IGMP entry on this window.
- **VLAN Name** – The name you have assigned to a specified VLAN.
- **Age-Out** – The time-out for entries on this table.
- **Delete** – Click this hyperlink to delete an IGMP entry on this window.

Spanning Tree

This section includes two windows, **STP Switch Settings** and **STP Port Settings**.

STP Switch Settings

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

Switch Spanning Tree Settings	
Spanning Tree Protocol	Disabled ▾
Time Since Topology Changes(Sec)	438
Topology Change Count	0
Bridge ID	8000003657000091
Designated Root	003657000091
Root Cost	0
Root Port	0
Bridge Max Age (6-40 Sec)	<input type="text" value="20"/>
Bridge Hello Time (1-10 Sec)	<input type="text" value="2"/>
Bridge Forward Delay (4-30 Sec)	<input type="text" value="15"/>
Bridge Priority (0-65535)	<input type="text" value="32768"/>
<input type="button" value="Apply"/>	
<i>Note: 2*(Forward Delay-1) >= Max Age,</i>	
<i>Max Age >= 2*(Hello Time +1)</i>	

Figure 7-8. Switch Spanning Tree Settings window

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

Parameters that you can change are:

- **Spanning Tree Protocol** – This drop-down menu allows you to enable the Spanning Tree Protocol setting.
- **Bridge Max Age (6-40 Sec) <20>** – The Maximum Age can be from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root 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) <2>** – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a Hello Time for your switch, and it is not the Root Bridge, the set Hello Time will be used if and when your switch becomes the Root Bridge.
- **Bridge Forward Delay (4-30 Sec) <15>** – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.
- **Bridge Priority (0-65535 Sec) <32768>** – A Bridge Priority can be from 0 to 65535. Zero is equal to the highest Bridge Priority.

STP Port Settings

Port	Connection	STP Status	Cost	Priority	Port State
1	100M/Full/None	Enabled	19	128	Forwarding
2	Nothing	Enabled	19	128	Disabled
3	Nothing	Enabled	19	128	Disabled
4	Nothing	Enabled	19	128	Disabled
5	Nothing	Enabled	19	128	Disabled
6	Nothing	Enabled	19	128	Disabled
7	Nothing	Enabled	19	128	Disabled
8	Nothing	Enabled	19	128	Disabled
9	Nothing	Enabled	19	128	Disabled
10	Nothing	Enabled	19	128	Disabled
11	Nothing	Enabled	19	128	Disabled
12	Nothing	Enabled	19	128	Disabled
13	Nothing	Enabled	19	128	Disabled
14	Nothing	Enabled	19	128	Disabled
15	Nothing	Enabled	19	128	Disabled
16	Nothing	Enabled	19	128	Disabled
17	Nothing	Enabled	19	128	Disabled
18	Nothing	Enabled	19	128	Disabled
19	Nothing	Enabled	19	128	Disabled
20	Nothing	Enabled	19	128	Disabled
21	Nothing	Enabled	19	128	Disabled
22	Nothing	Enabled	19	128	Disabled
23	Nothing	Enabled	19	128	Disabled
24	Nothing	Enabled	19	128	Disabled

Figure 7-9. STP Port Settings window

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

The information on the window is described as follows:

- **From** – Enter the first port to be configured.
- **To** – Enter the last port to be configured.
- **State** – The Spanning Tree Protocol state for a selected port can either be *Enabled* or *Disabled*.
- **Cost (1~65535)** – A port cost can be set between 1 and 65535. The lower the cost, the greater the probability the port will be chosen as the designated port (chosen to forward packets).
- **Priority (0~255)** – A port priority can be set from 0 to 255. The lower the priority, the greater the probability the port will be chosen as the root port.

Static Forwarding Table

Static Unicast Forwarding

Add Static Forwarding

MAC Address	VID	Type	PortMap												Apply									
			1	2	3	4	5	6	7	8	9	10	11	12										
			13	14	15	16	17	18	19	20	21	22	23	24										
<input type="text"/>	<input type="text"/>	Permanent	<input checked="" type="radio"/>	<input type="button" value="Apply"/>																				

Static Forwarding Table

MAC Address	VID	Type	PortMap												Remove									
			1	2	3	4	5	6	7	8	9	10	11	12										
			13	14	15	16	17	18	19	20	21	22	23	24										

Figure 7-10. Add Static Forward window

The window above allows you to set up static packet forwarding on the switch.

The information on the window is described as follows:

- **MAC Address** – The MAC address from which packets will be statically filtered.
- **VID** – The VLAN ID number of the VLAN to which the MAC address belongs.
- **Type** – Select the filter type, *Permanent* or *DeleteOnReset*.
- **Port Map** – Allows the designation of the port on which the above MAC address resides.

Static Multicast Forwarding

Add Multicast Forwarding

MAC Address	VID	Type	PortMap																								Apply	
			State	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23		24
			None	<input checked="" type="radio"/>		<input checked="" type="radio"/>																						
<input type="text"/>	<input type="text"/>	Permanent	Egress	<input type="radio"/>	<input type="radio"/>	<input type="button" value="Apply"/>																						

Multicast Forwarding Table Entries: 0

MAC Address	VID	Type	PortMap																								Remove	
			State	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23		24
			None																									
			Egress																									

Figure 7-11. Add Multicast Forwarding window

The information on the window is described as follows:

- **MAC Address** – The MAC address of the static source of multicast packets.
- **VID** – The VLAN ID number of the VLAN to which the MAC address belongs.
- **Type** – Select the filter type, *Permanent* or *DeleteOnReset*.

- **Port Map** – Allows the selection of ports that will be members of the static multicast group and ports that have no restrictions from joining dynamically.

VLANs

This section includes **Static VLAN Entry** and **Port VLAN ID (PVID)**.

Static VLAN Entry

802.1Q Static VLANs Entries: 1			
VLAN ID (VID)	VLAN Name	New	Delete
1	DEFAULT_VLAN		

Figure 7-12. 802.1Q Static VLANs window

To add an entry to this table, click New and then fill in the appropriate information in the window below. To delete an entry, click the icon in the Delete column.

802.1Q Static VLAN Setup

VID:

VLAN Name:

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag	<input checked="" type="checkbox"/>																							
None	<input type="checkbox"/>																							
Egress	<input checked="" type="checkbox"/>																							
Forbidden	<input type="checkbox"/>																							

Figure 7-13. 802.1Q Static VLAN Setup window

To add an 802.1Q static VLAN entry, enter the desired VLAN ID number in the first field and then enter a VLAN name in the second field. Next, either check the Tag option, or leave it unchecked if you don't want a member port to be a *Tagging* port. In the last two rows, None should be checked if you don't want a port to belong to the VLAN. Otherwise, check Egress to statically set a port to belong to a VLAN or Forbidden to prevent a port from being a member of the VLAN. Click **Apply** to let the changes take effect.

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag	<input type="checkbox"/>																							
None	<input type="radio"/>																							
Egress	<input checked="" type="radio"/>																							
Forbidden	<input type="radio"/>																							

Figure 7-14. 802.1Q Static VLAN Setup window

To modify an entry, click the pointer icon next to the appropriate table entry on the **802.1Q Static VLANs** window and then complete the appropriate information on the window above. Click **Apply** to let your changes take effect.

To delete an entry, click the X icon next to the appropriate table entry on the **802.1Q Static VLANs** window and then click **Apply**.

The information on the window is described as follows:

- **VLAN ID (VID)** – The VLAN ID of the VLAN that is being created.
- **VLAN Name** – The name of the VLAN that is being created.
- **Tag** – Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
- **None** – Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
- **Egress** – Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.
- **Forbidden** – Specifies the port that is not allowed to be a member of the VLAN.

Port VLAN ID (PVID)

802.1Q Port Settings

From	To	PVID	Ingress	GVRP	Apply
Port 1 ▾	Port 1 ▾	1	Off ▾	Off ▾	Apply

802.1Q Port Table

Port	PVID	Ingress	GVRP
1	1	OFF	ON
2	1	OFF	ON
3	1	OFF	ON
4	1	OFF	ON
5	1	OFF	ON
6	1	OFF	ON
7	1	OFF	ON
8	1	OFF	ON
9	1	OFF	ON
10	1	OFF	ON
11	1	OFF	ON
12	1	OFF	ON
13	1	OFF	ON
14	1	OFF	ON
15	1	OFF	ON
16	1	OFF	ON
17	1	OFF	ON
18	1	OFF	ON
19	1	OFF	ON
20	1	OFF	ON
21	1	OFF	ON
22	1	OFF	ON
23	1	OFF	ON
24	1	OFF	ON
End of data!			

Figure 7-15. 802.1Q Port Settings window

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

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

create and manage VLANs on switches connected through 802.1Q ports. Click **Apply** to let your changes take effect.

The information on the window is described as follows:

- **PVID** – PVID is used to decide whether received tagged packets belong to a VLAN.
- **Ingress** – Ingress filtering is used to check if the received port is a member port of the VLAN whose VID is equal to the VID of incoming packets.
- **GVRP** – For each corresponding port, GARP VLAN Registration Protocol can be *Enabled* or *Disabled*.

Port Default Priority

Default Port Priority assignment

From	To	Priority(0~7)	Apply
Port 1 ▾	Port 1 ▾	<input type="text" value="0"/>	<input type="button" value="Apply"/>

The Port Priority Table

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0

Figure 7-16. Default Port Priority assignment window

This window allows you to set a default priority for packets that have not already been assigned a priority value. After filling out the two fields offered, click **Apply** to let your changes take effect.

Class of Traffic

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

Apply

Figure 7-17. Traffic Class Configuration window

This window allows you to configure traffic class priority by specifying the class value, from 0 to 3, of the switch's eight levels of priority. Click **Apply** to let your changes take effect.

Class of Service

Class of Service Configuration		
	Max. Packets	Port Maxlimit Drop
Class-0	No Limit	
Class-1	No Limit	
Class-2	No Limit	
Class-3	No Limit	
Max. Latency	3.2 s	

Apply

Figure 7-18. Class of Service Configuration window

This window allows you to set the following features:

- **Max. Packets** – The Class of Service scheduling algorithm starts from the highest CoS for a given port, sends the maximum number of packets, then moves on to the next lower CoS. The values that

can be entered in this field are from 1 to 255. Entering zero instructs the switch to continue processing packets until there are no more packets in the CoS transaction queue.

- **Max. Latency** – The maximum allowable time a packet will stay in the CoS queue, in microseconds and seconds. The packets in this queue are not delayed more than the maximum allowable latency entered in this field. Maximum latency takes precedence over the CoS scheduling algorithm.

Click the pointer icon in the Port Maxlimit Drop column at the top of the window above to set the port queue priority for each class:

Port Maxlimit Drop Settings: Queue 0

From	To	Class State	Apply
Port 1 ▾	Port 1 ▾	Off ▾	Apply

Port Class Table

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

Figure 7-19. Port Maxlimit Drop Settings window

The switch divides the buffer into four parts: *Queue0*, *Queue1*, *Queue2*, and *Queue3*. *Queue0* is the highest priority and *Queue3* is the lowest. Use the window above to select the ports for each of the four queue priorities. Turn the Class State to *On* for the specified range of ports and then click **Apply** to let your changes take effect.

RS232 & SLIP

Serial Port Settings	
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Auto-Logout	Never
Serial Port For	Console

SLIP Settings	
Interface Name	
Local IP Address	0.0.0.0
Remote IP Address	0.0.0.0
MTU	1006

Figure 7-20. Serial Port Settings window

The following fields can then be set:

- **Baud Rate:**<9600> – Sets the serial bit rate that will be used to communicate the next time the switch is restarted. Available speeds are 2400, 9600, 19200, 38400 and 115200 bits per second. The default setting is 9600.
- **Data Bits:**<8> – Select 7 or 8. The default is 7.
- **Parity:**<None> – Choose from *None*, *Even* or *Odd*. The default is *None*.
- **Stop Bits:**<1> – Select 1 or 2. The default is 1.
- **Auto-Logout:**<Never> – This sets the time the interface can be idle before the switch automatically logs-out the user. The options are 2 mins, 5 mins, 10 mins, 15 mins, or *Never*.
- **Serial Port For:**<Console> – Change this field to *SLIP* and enter the appropriate information in the **Interface Name**, **Local IP Address**, **Remote IP Address**, and **MTU** fields which become active once *SLIP* is selected.

Management

This category includes: **Security IP**, **SNMP Manager**, **Trap Manager**, and **User Accounts**.

Security IP

Security IP Management		
IP1 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP2 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP3 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP4 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP5 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP6 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP7 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP8 Access to Switch	<input type="text" value="0.0.0.0"/>	

Note: Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

Figure 7-21. Security IP Management window

Use this window to specify IP addresses that are allowed to access the switch.

SNMP Manager

SNMP Manager Configuration		
Community String	Access Right	Status
<input type="text" value="public"/>	<input type="text" value="Read-Only"/>	<input type="text" value="Valid"/>
<input type="text" value="private"/>	<input type="text" value="Read-Write"/>	<input type="text" value="Valid"/>
<input type="text"/>	<input type="text" value="Read-Only"/>	<input type="text" value="Invalid"/>
<input type="text"/>	<input type="text" value="Read-Only"/>	<input type="text" value="Invalid"/>

Figure 7-22. SNMP Manager Configuration window

To use the functions on this window, enter the appropriate SNMP information. You may enter up to four entries. Click **Apply** to put the settings into effect.

The Community String 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.
- **Status** – Option to set the current community string to *Valid* or *Invalid*.

Trap Manager

Trap Receiving Station	Community String	Status
0.0.0.0		Invalid

Apply

Figure 7-23. SNMP Trap Manager Configuration window

A trap receiving station is a device that constantly runs a network management application to receive and store traps. You may enter up to four entries. Click **Apply** to put the settings into effect.

The information is described as follows:

- **Trap Receiving Station** – The IP address of the trap receiving station.
- **Community String** – A user-defined SNMP community name.
- **Status** – Option to set the trap receiving station to *Valid* or *Invalid*.

User Accounts

The Switch allows you to set up and manage user accounts in the following two windows.

User Account Management

User Name	Access Right	New
-----------	--------------	-----

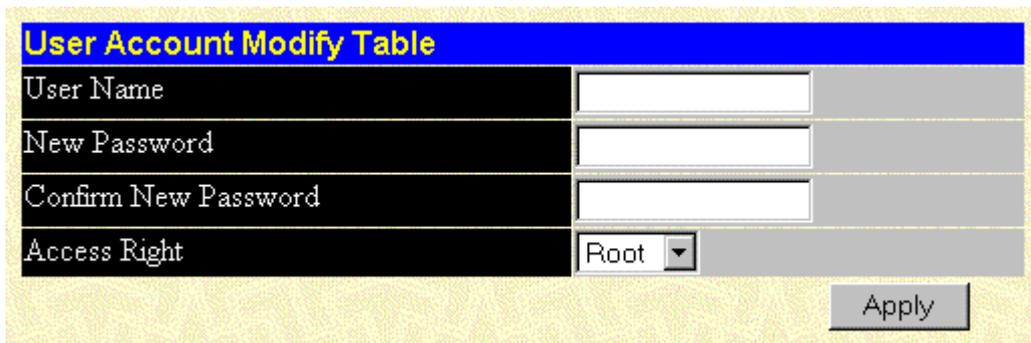
Figure 7-24. User Account Management window

The information on the window is described as follows:

- **User Name** – Displays all current users for the switch.

- **Access Right** – Displays the current access level assigned to each corresponding user. There are three access levels: *User*, *User+*, and *Root*. A *Root* user has full read/write access, while a *User* has read only access. A *User+* has the same privileges as a *User*, but with the added ability to restart the switch.
- **New** – Select this hyperlink to add a new user to the table.

User Account Modify Table



User Account Modify Table	
User Name	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
Access Right	Root <input type="button" value="v"/>

Figure 7-25. User Account Modify Table window

To add or delete a User Account, fill in the appropriate information in the User Name, New Password, and Confirm New Password fields. Then select the desired access, *Root*, *User* or *User+*, in the **Access Right** control and click **Apply**.

The information on the window is described as follows:

- **User Name** – Enter a user name in this field.
- **New Password** – Enter the desired new password in this field.
- **Confirm New Password** – Enter the new password a second time.
- **Access Right** – Displays the current access level assigned to each corresponding user. There are three access levels: *User*, *User+*, and *Root*. A *Root* user has full read/write access, while a *User* has read only access. A *User+* has the same privileges as a *User*, but with the added ability to restart the Switch.

Monitoring

This category includes: **Port Utilization**, **Packets (Received (RX), UMB_cast (RX), and Transmitted (TX))**, **Errors (Received (RX) and Transmitted (TX))**, **Size (Received (RX))**, **MAC Address Table**, **IGMP Snooping Table**, **VLAN Multicast Table**, **IGMP Multicast Table**, and **VLAN Status Table**, and secondary windows.

Port Utilization

The Switch can display the utilization percentage of a specified port in the window below.

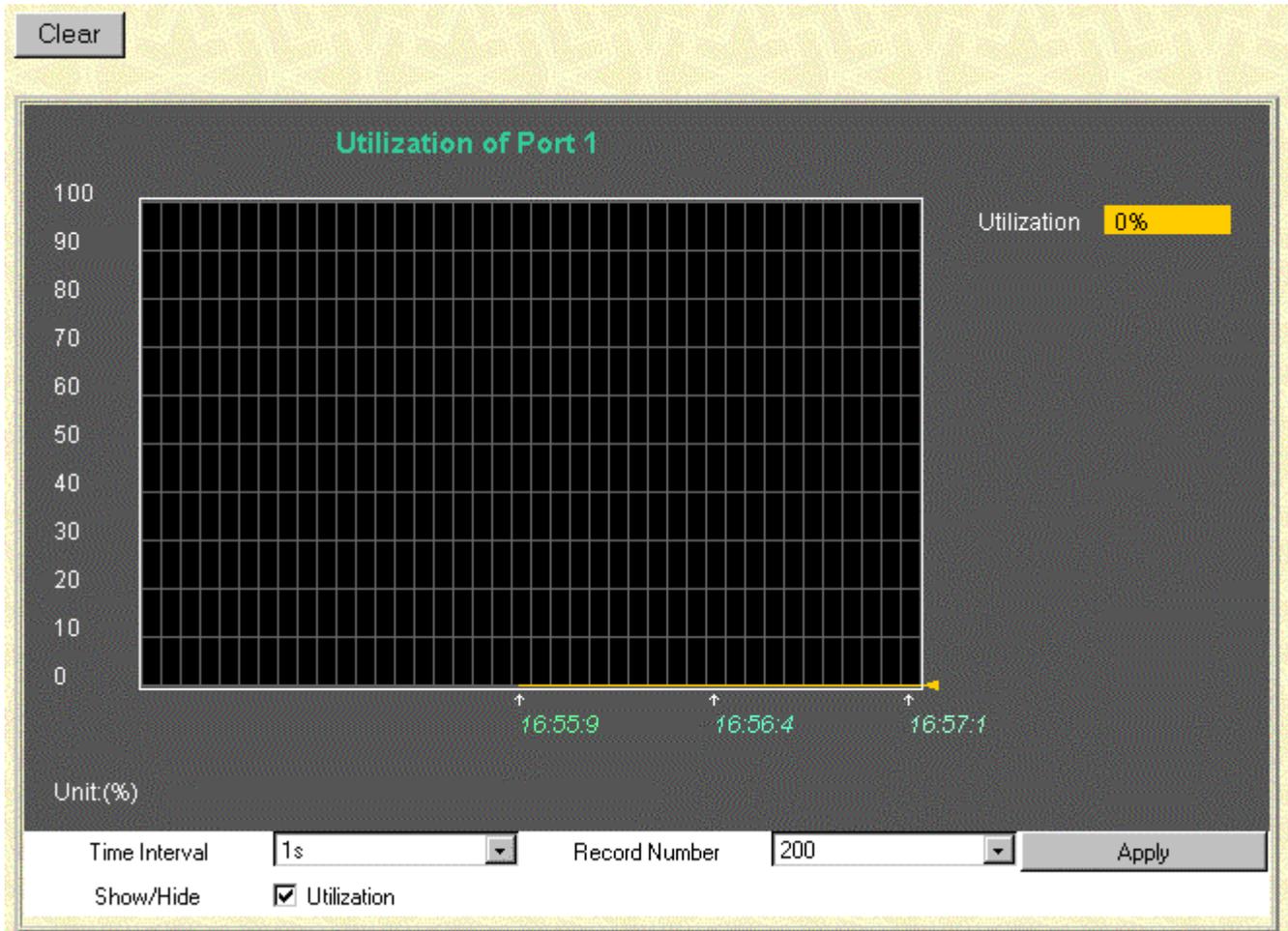


Figure 7-26. Utilization of Port window

The information is described as follows:

- **Time Interval** – Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is one second.
- **Record Number** – Select number of times the switch will be polled between *20* and *200*. The default value is 20.
- **Show/Hide** – Check whether or not to display Utilization.
- **Clear** – Clicking this button clears all statistics counters on this window.

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. The six windows offered are as follows:

Received (RX)

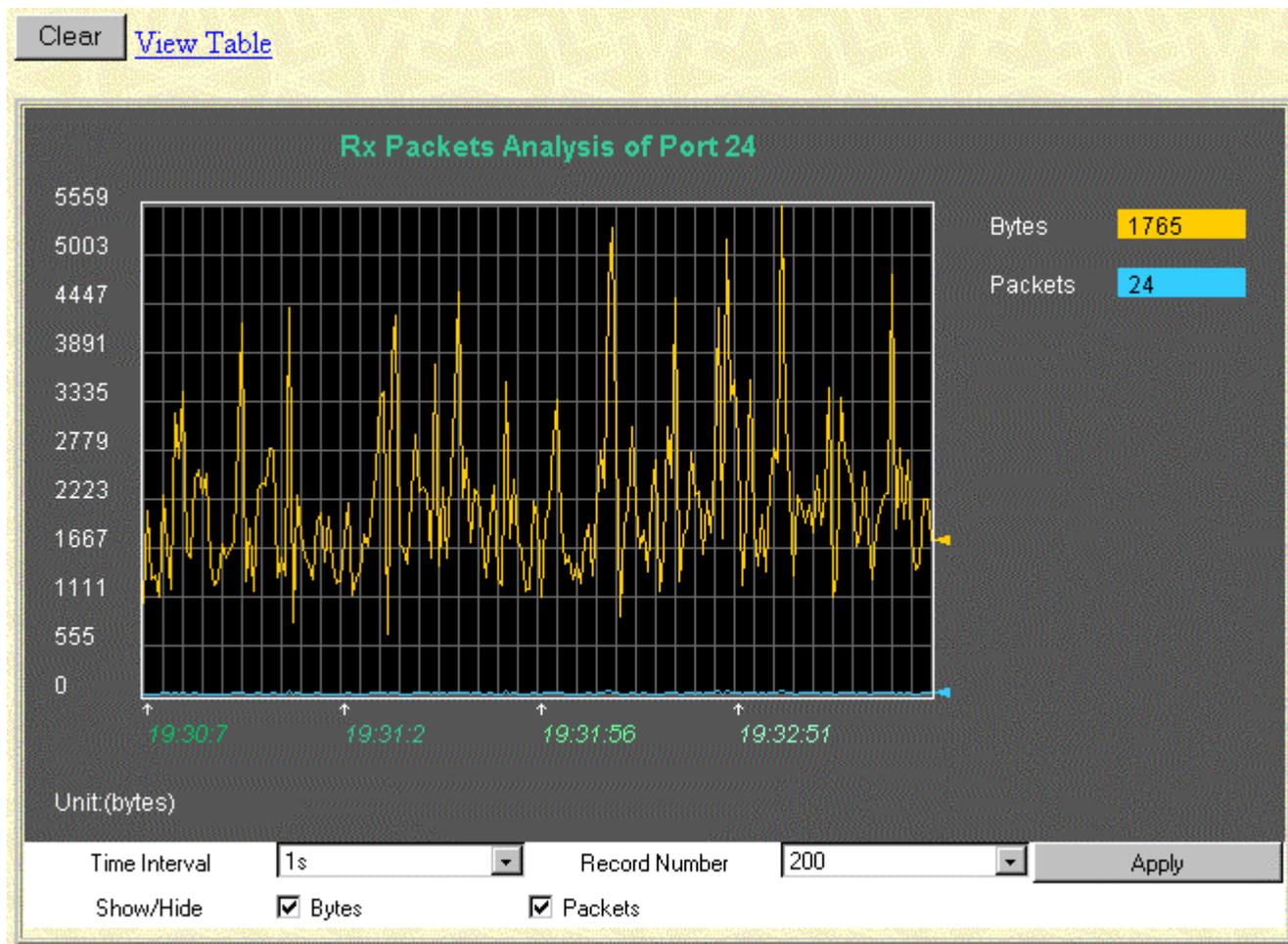


Figure 7-27. Rx Packets Analysis window (Line Chart)

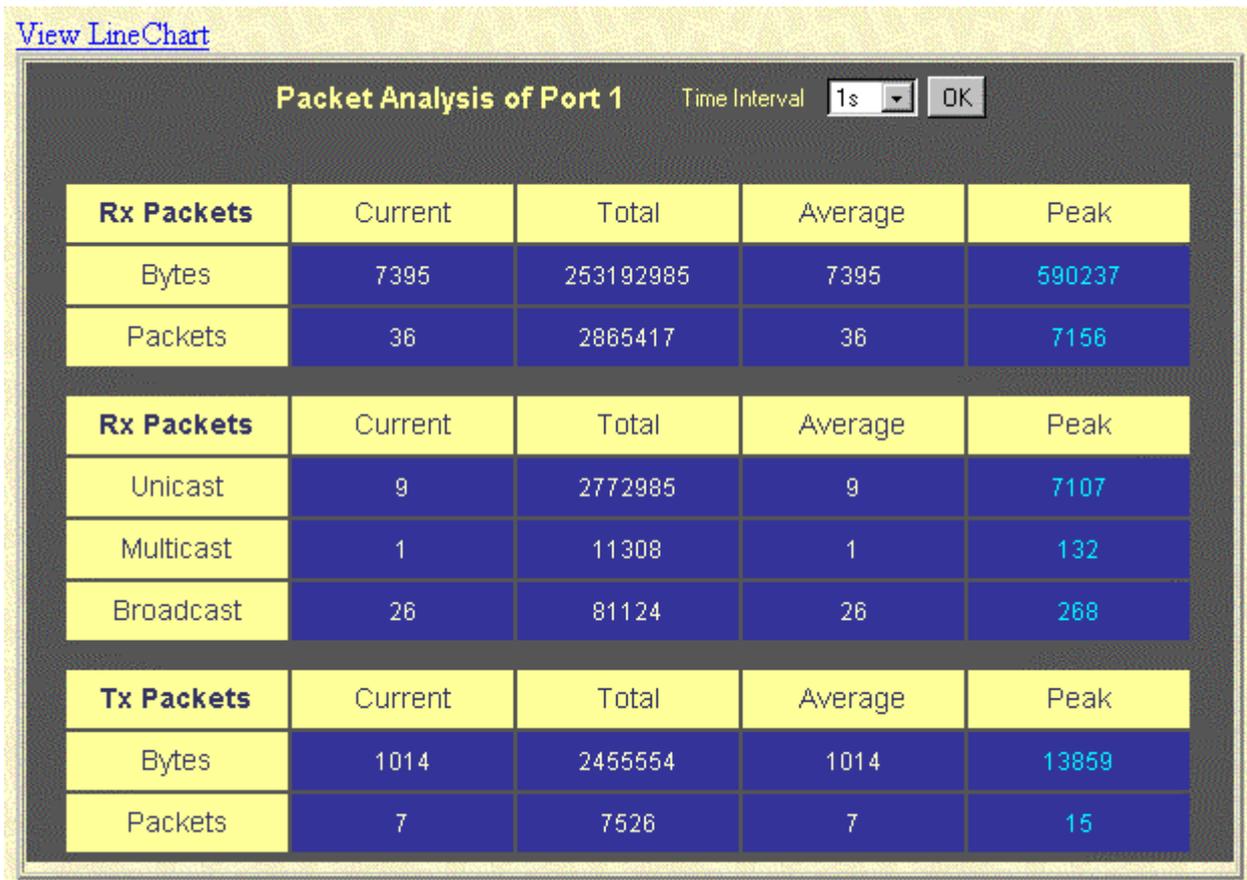


Figure 7-28. Rx Packets Analysis window (Table)

The information is described as follows:

- **Time Interval** – Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is one second.
- **Record Number** – Select number of times the switch will be polled between *20* and *200*. The default value is *20*.
- **Bytes** – Counts the number of bytes received on the port.
- **Packets** – Counts the number of packets received on the port.
- **Show/Hide** – Check whether or not to display Bytes and Packets.
- **Clear** – Clicking this button clears all statistics counters on this window.
- **View Table** – Clicking this button instructs the switch to display a table rather than a line graph.
- **View Line Chart** – Clicking this button instructs the switch to display a line graph rather than a table.

UMB-cast (RX)

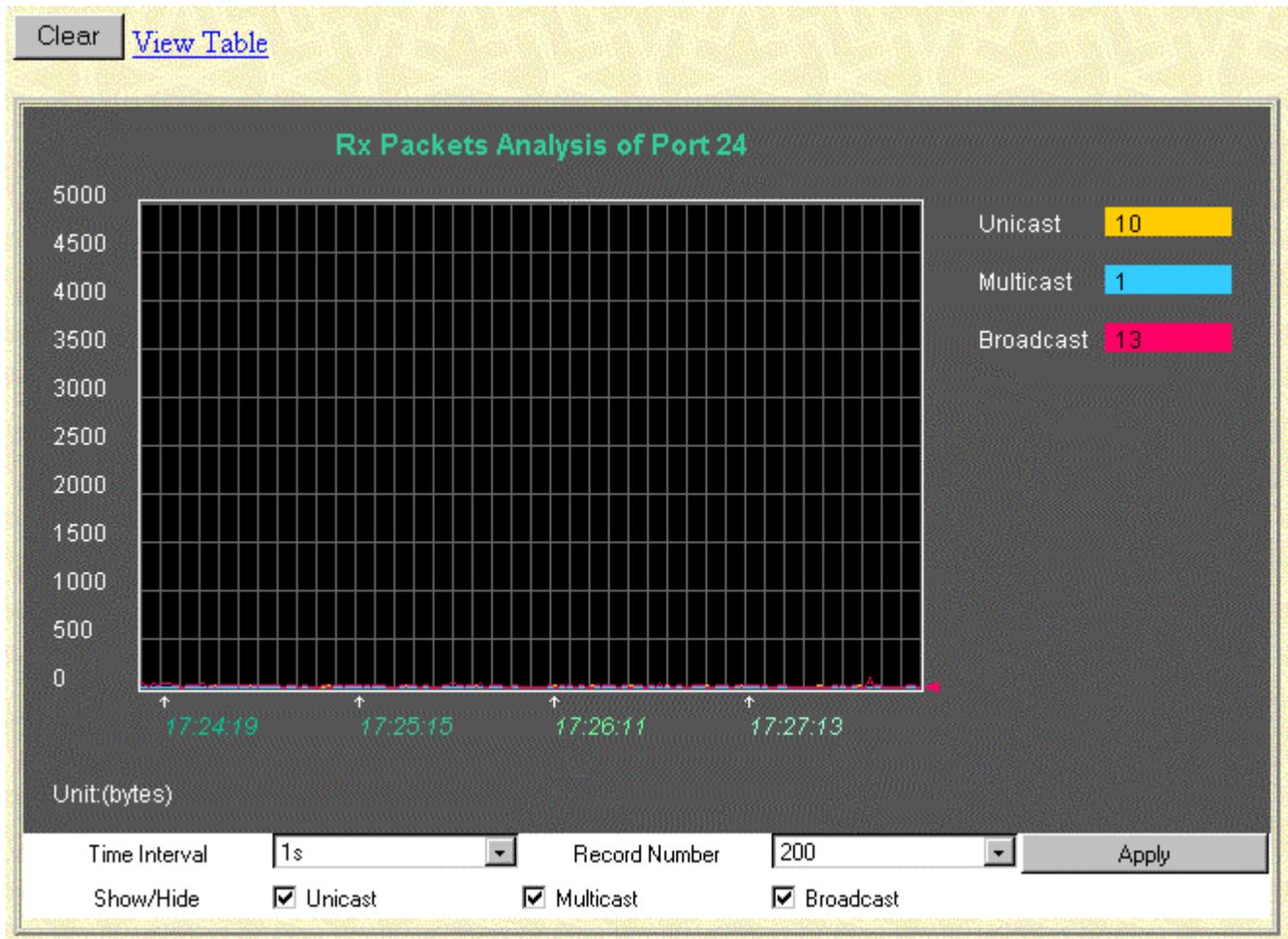


Figure 7-29. Rx Packets Analysis window for UMB_cast (Line Chart)

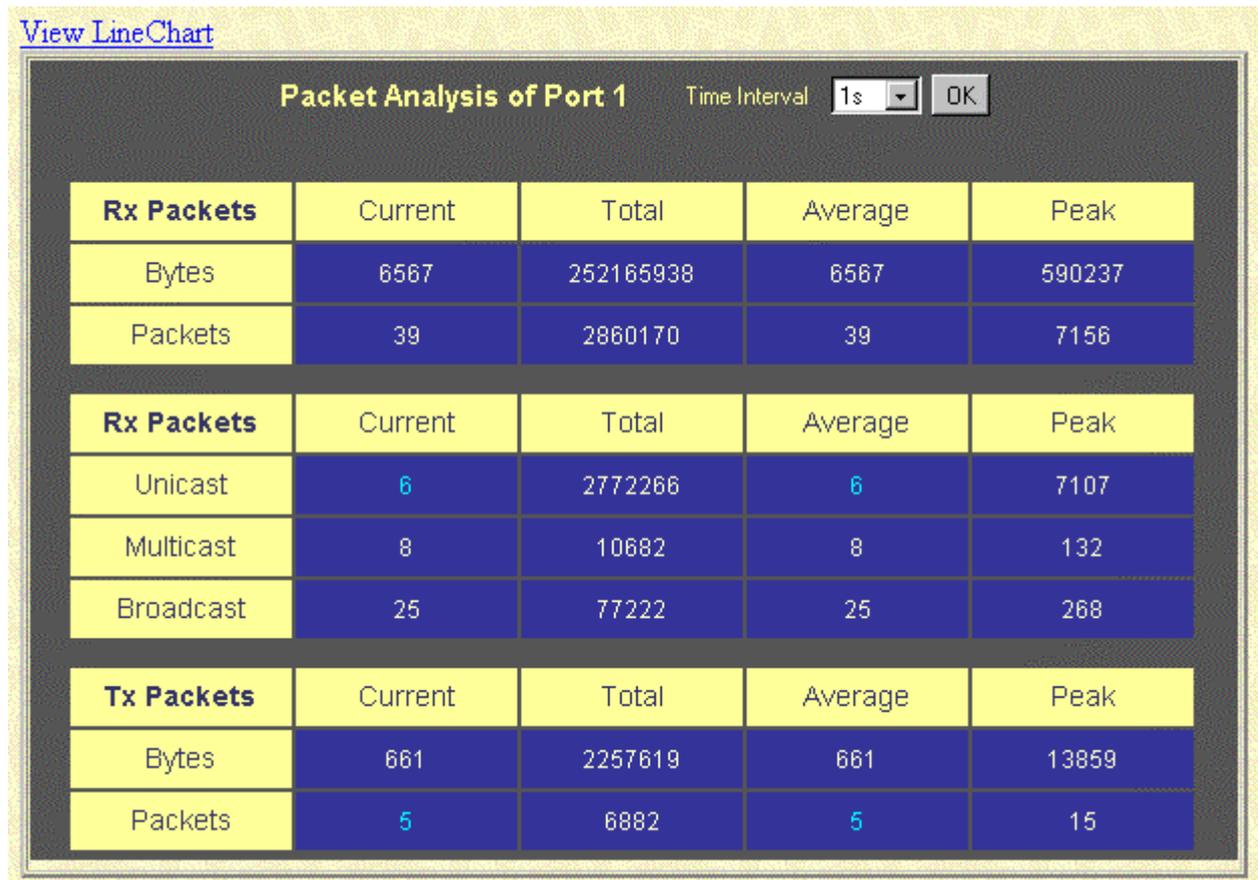


Figure 7-30. Rx Packets Analysis window for UMB_cast (Table)

The information is described as follows:

- **Time Interval** – Select the desired setting between *1s* and *60s*, where “s” stands for seconds.
- **Record Number** – Select number of times the switch will be polled between *20* and *200*.
- **Multicast** – Counts the total number of good packets that were received by a multicast address.
- **Broadcast** – Counts the total number of good packets that were received by a broadcast address.
- **Unicast** – Counts the total number of good packets that were received by a unicast address.
- **Show/Hide** – Check whether or not to display Multicast, Broadcast, and Unicast Packets.
- **Clear** – Clicking this button clears all statistics counters on this window.
- **View Table** – Clicking this button instructs the switch to display a table rather than a line graph.
- **View Line Chart** – Clicking this button instructs the switch to display a line graph rather than a table.

Transmitted (TX)

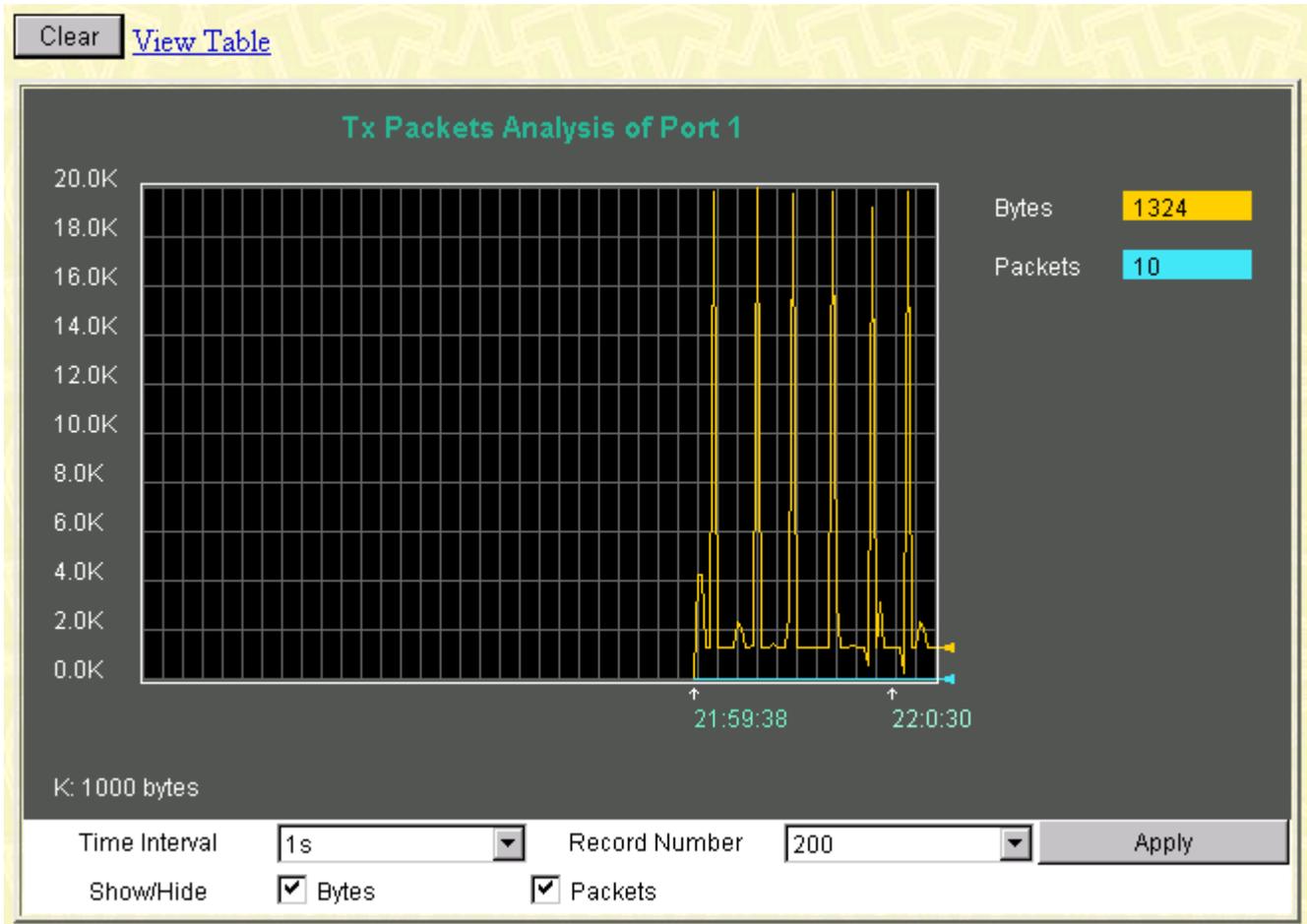


Figure 7-31. Tx Packets Analysis window (Line Chart)

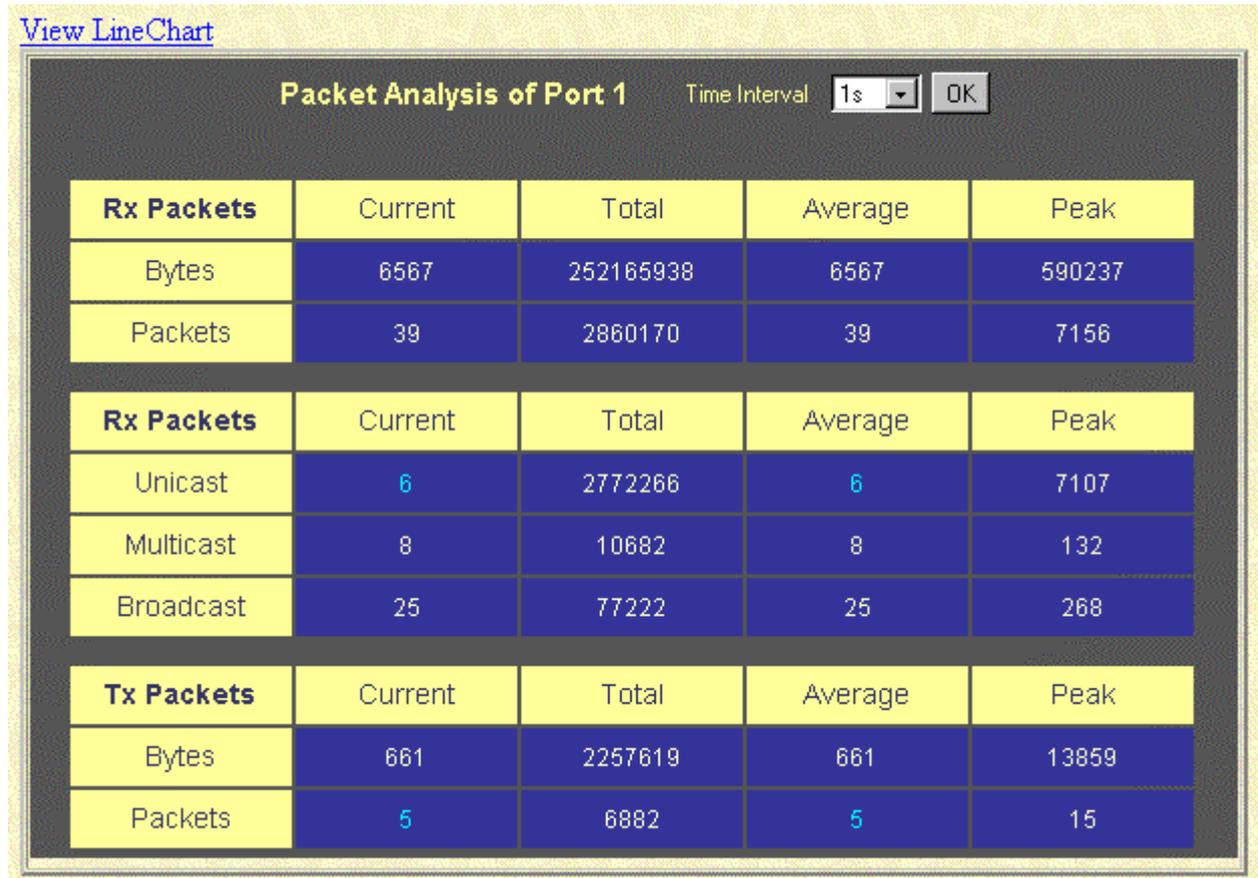


Figure 7-32. Tx Packets Analysis window (Table)

The information is described as follows:

- **Time Interval** – Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is one second.
- **Record Number** – Select number of times the switch will be polled between *20* and *200*. The default value is 20.
- **Bytes** – Counts the number of bytes successfully sent from the port.
- **Packets** – Counts the number of packets successfully sent on the port.
- **Show/Hide** – Check whether or not to display Bytes and Packets.
- **Clear** – Clicking this button clears all statistics counters on this window.
- **View Table** – Clicking this button instructs the switch to display a table rather than a line graph.
- **View Line Chart** – Clicking this button instructs the switch to display a line graph rather than a table.

Errors

The Web Manager allows port error statistics compiled by the switch's management agent to be viewed as either a line graph or a table. The four windows offered are as follows:

Received (RX)

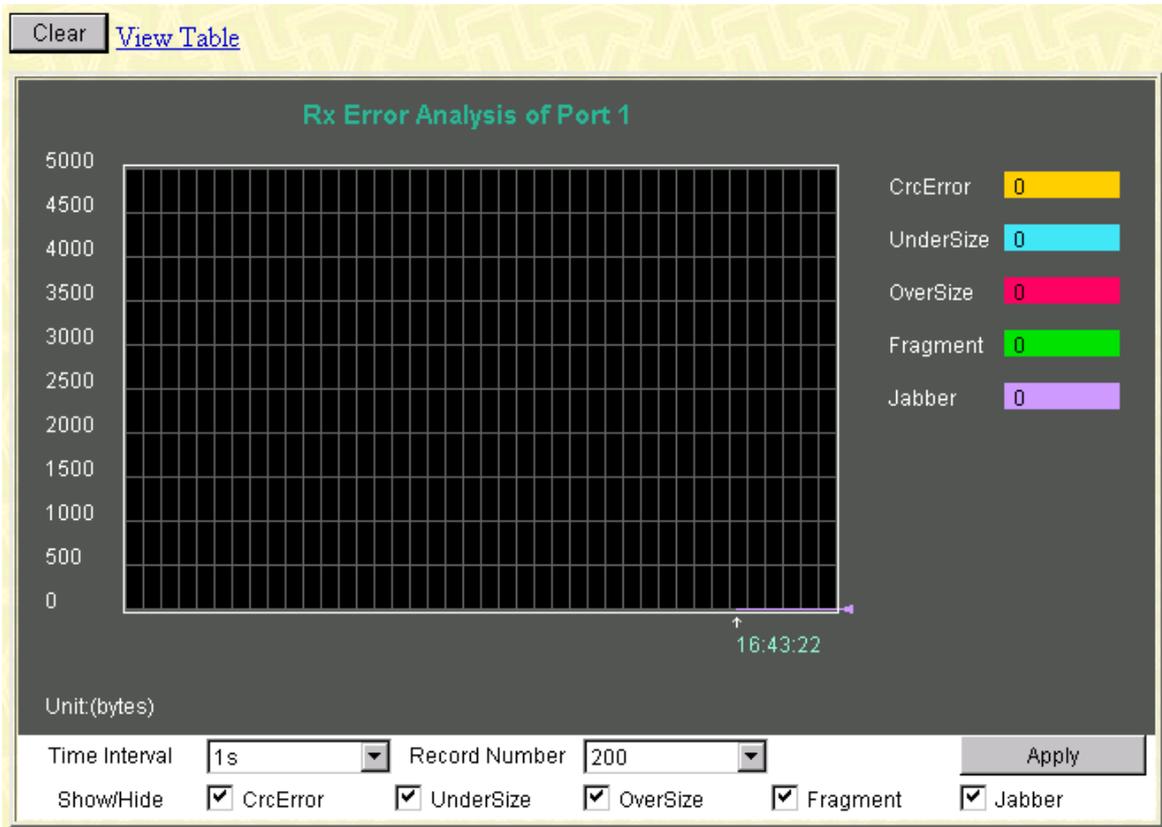


Figure 7-33. Rx Error Analysis window (Line Chart)

[View LineChart](#)

Packet Analysis of Port 1 Time Interval: 1s OK

Rx Error	Current	Total	Average	Peak
CrcError	0	0	0	0
UnderSize	0	0	0	0
OverSize	0	0	0	0
Fragment	0	0	0	0
Jabber	0	0	0	0

Figure 7-34. Rx Error Analysis window (Table)

The information is described as follows:

- **Time Interval** – Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is one second.
- **Record Number** – Select number of times the switch will be polled between *20* and *200*. The default value is *20*.
- **CRCError** – Counts otherwise valid frames that did not end on a byte (octet) boundary.
- **UnderSize** – The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
- **OverSize** – Counts packets received that were longer than 1518 octets, or if a VLAN frame, 1522 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
- **Fragment** – The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
- **Jabber** – The number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
- **Show/Hide** – Check whether or not to display CrcError, UnderSize, OverSize, Fragment, Jabber, and Drop errors.
- **Clear** – Clicking this button clears all statistics counters on this window.
- **View Table** – Clicking this button instructs the switch to display a table rather than a line graph.
- **View Line Chart** – Clicking this button instructs the switch to display a line graph rather than a table.

Transmitted (TX)

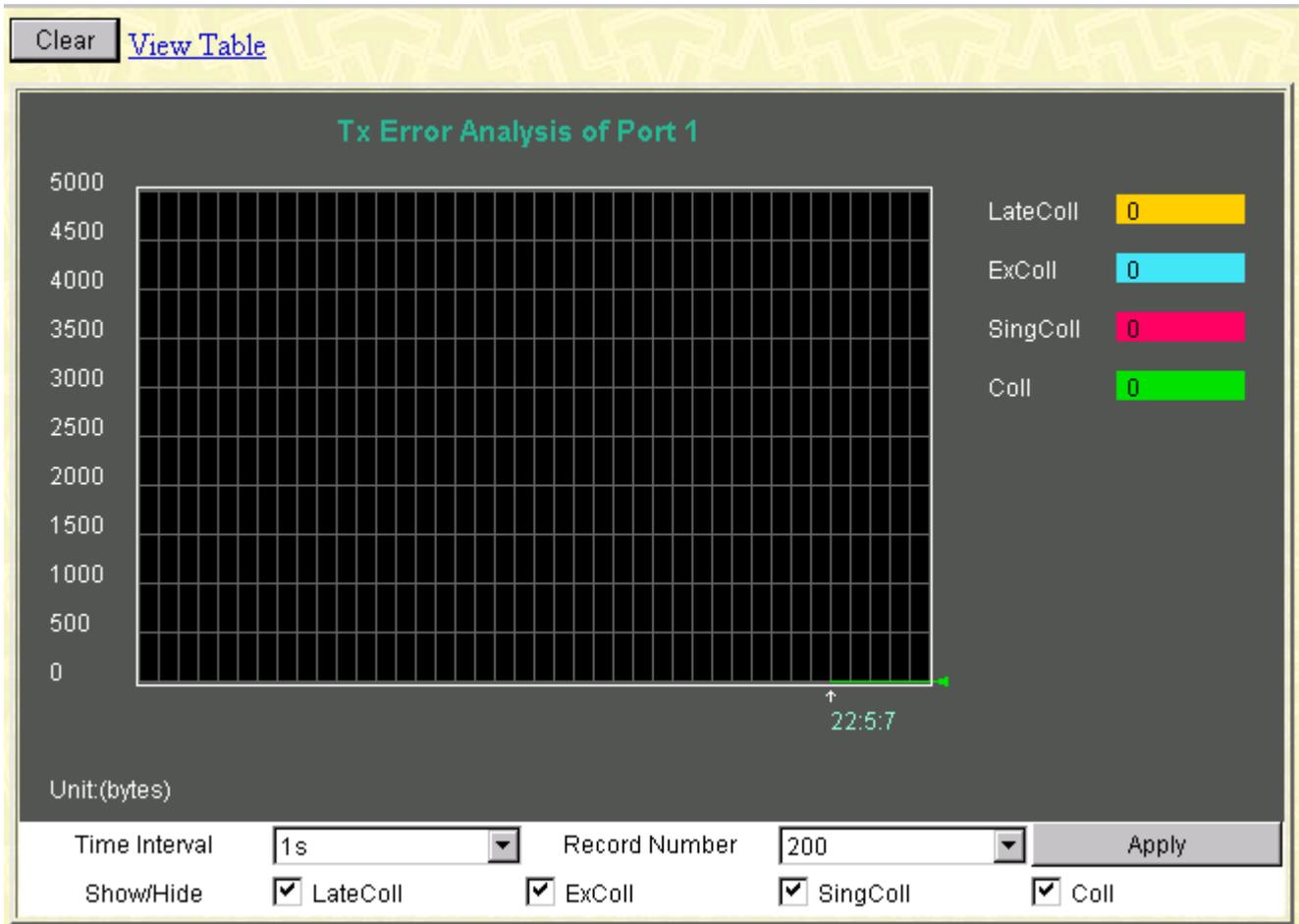


Figure 7-35. Tx Error Analysis window (Line Chart)

[View LineChart](#)

Packet Analysis of Port 1 Time Interval

Tx Error	Current	Total	Average	Peak
LateColl	0	0	0	0
ExColl	0	0	0	0
SingColl	0	0	0	0
Coll	0	0	0	0

Figure 7-36. Packet Analysis window (Table)

The information is described as follows:

- **Time Interval** – Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is one second.
- **Record Number** – Select number of times the switch will be polled between *20* and *200*. The default value is *20*.
- **LateColl** – Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
- **ExColl** – Counts the number of frames that experienced 16 collisions during transmission and were aborted.
- **SingColl** – Counts the number of frames transmitted that experienced exactly one collision during transmission.
- **Coll** – Counts the number of collisions experienced during the transmission of a frame as defined as the simultaneous presence of signals on the DO and RD circuits, i.e. transmitting and receiving at the same time.
- **Show/Hide** – Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.
- **Clear** – Clicking this button clears all statistics counters on this window.
- **View Table** – Clicking this button instructs the switch to display a table rather than a line graph.
- **View Line Chart** – Clicking this button instructs the switch to display a line graph rather than a table.

Size

The Web Manager allows packets transmitted and received by the switch, arranged in six groups, to be viewed as either a line graph or a table. The two windows offered are as follows:

Packet Size

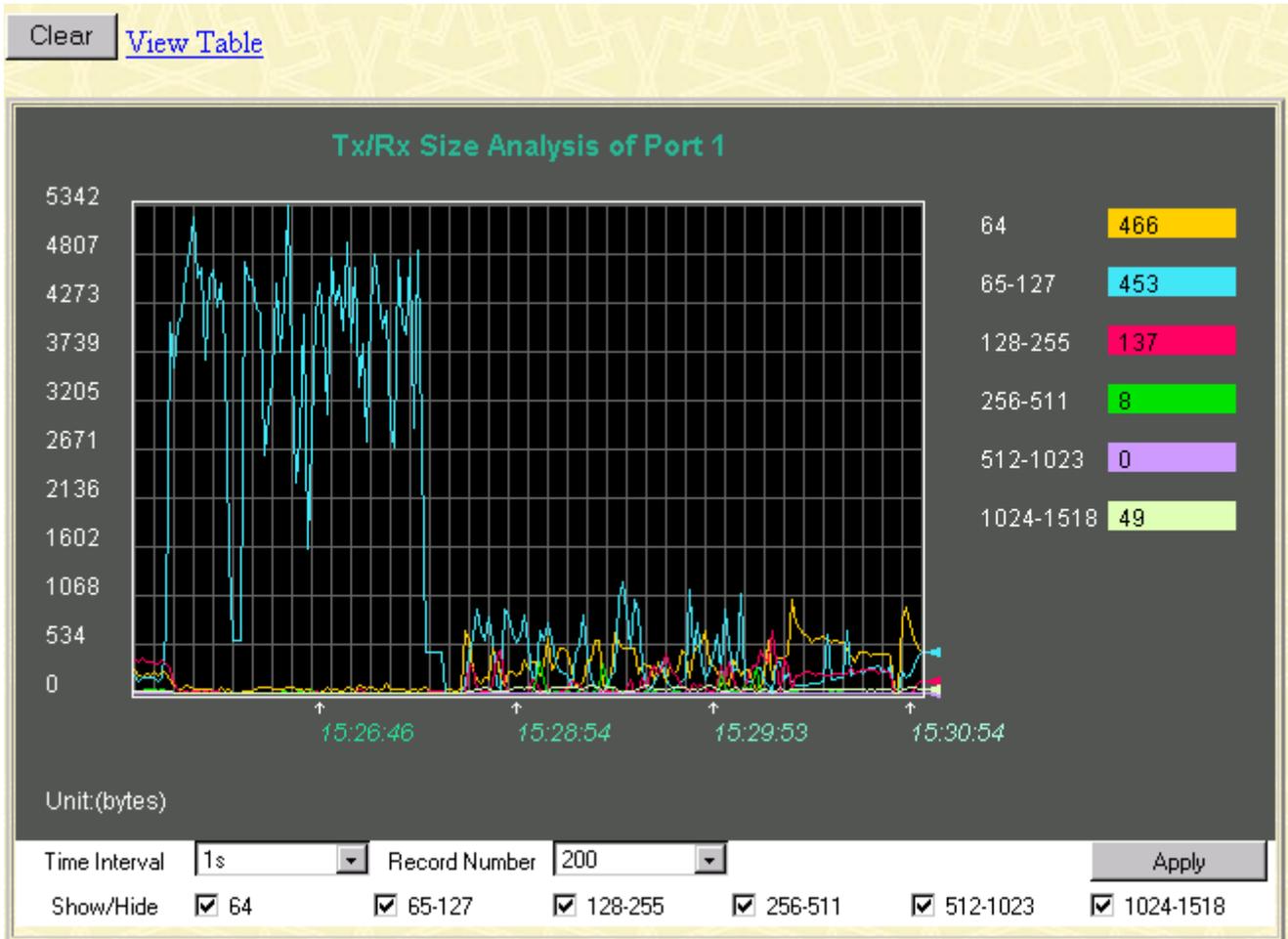


Figure 7-37. Tx/Rx Size Analysis window (Line Chart)

[View Line Chart](#)

Tx/Rx Size	Current	Total	Average	Peak
64	455	1313292	455	1030
65-127	494	2463416	494	5342
128-255	188	1433496	188	690
256-511	15	279128	15	349
512-1023	0	5841	0	18
1024-1518	35	206572	35	90

Figure 7-38. Packet Analysis window (Table)

The information is described as follows:

- **Time Interval** – Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is one second.
- **Record Number** – Select number of times the switch will be polled between *20* and *200*. The default value is 20.
- **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).
- **Show/Hide** – Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
- **Clear** – Clicking this button clears all statistics counters on this window.

- **View Table** – Clicking this button instructs the switch to display a table rather than a line graph.
- **View Line Chart** – Clicking this button instructs the switch to display a line graph rather than a table.

MAC Address Table

The Web Manager allows the switch's MAC address table (sometimes referred to as a forwarding table) to be viewed:

The screenshot shows the MAC Address Table window with the following search filters and table data:

Search by VLAN ID	Search by MAC Address	Search by Port	Jump	Find
<input type="text"/>	<input type="text" value="00-00-00-00-00-00"/>	<input type="text" value="13"/>	<input type="button" value="Jump"/>	<input type="button" value="Find"/>
		<input type="button" value="Clear All"/>	<input type="button" value="Clear By Port"/>	

MAC Address Table			
VID	MAC Address	Port	Learned
1	00-00-00-00-00-05	15	dynamic
1	00-00-81-9a-a0-9f	15	dynamic
1	00-00-81-9a-f2-ba	15	dynamic
1	00-00-81-9a-f2-f4	15	dynamic
1	00-00-86-47-47-58	15	dynamic
1	00-00-86-4e-e1-01	15	dynamic
1	00-00-e2-41-fb-54	15	dynamic
1	00-00-f4-95-b5-4a	15	dynamic
1	00-00-f8-7c-1c-29	15	dynamic
1	00-01-02-03-04-00	15	dynamic
1	00-01-02-42-41-00	15	dynamic
1	00-01-03-83-0e-ea	15	dynamic
1	00-01-03-83-11-fd	15	dynamic
1	00-01-30-fa-5f-00	15	dynamic
1	00-01-96-9c-06-00	15	dynamic
1	00-01-fd-14-14-00	15	dynamic
1	00-02-a5-d1-00-b8	15	dynamic
1	00-03-6d-1e-76-79	15	dynamic
1	00-05-5d-06-57-26	15	dynamic
1	00-05-5d-10-11-63	15	dynamic

Total Addresses in Table: 462

Figure 7-39. MAC Address Table window

The information is described as follows:

- **Search by VLAN ID** – Allows the forwarding table to be browsed by VLAN ID (VID).
- **Search by MAC Address** – Allows the forwarding table to be browsed by MAC Address.
- **Search by Port** – Allows the forwarding table to be browsed by port number.
- **Jump** – Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
- **Find** – Click the icon to find the data entry.
- **Clear All** – Clears all forwarding table entries.
- **Clear By Port** – Clears the forwarding table entries that have the entered port number.
- **VID** – The VLAN ID of the VLAN the port is a member of.
- **MAC Address** – The MAC address entered into the address table.
- **Port** – The port that the MAC address above corresponds to.
- **Learned** – How the switch discovered the MAC address. The possible entries are *Dynamic*, *Self*, and *Static*.
- **Next** – Click this button to view the next page of the address table.

IGMP Snooping Table

The switch's IGMP snooping table can be browsed using the Web Manager. The table is displayed by VLAN ID (VID).

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

Figure 7-40. IGMP Snooping Table window

The information is described as follows:

- **VID** –VLAN ID of the VLAN for which the IGMP Snooping table is to be displayed.
- **Search** – Click on this button to display the IGMP Snooping Table for the current VID.
- **Multicast Group** – The IP address of a multicast group learned by IGMP snooping.
- **MAC Address** – The corresponding MAC address learned by IGMP snooping.
- **Port Map** – Displays the ports that have forwarded multicast packets.
- **Reports** – The number of IGMP reports for the listed source.

VLAN Multicast Table

This read-only table displays the VLAN multicast table for each VLAN ID on the switch.

VLAN Multicast Table																									
VID	Multicast Group	Static Port List																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
End of data!																									

Figure 7-41. VLAN Multicast Table window

IGMP Multicast Table

This read-only table displays the IGMP multicast table for each VLAN ID on the switch.

IGMP Multicast Table																									
VID	Multicast Group	IGMP Snooping Port List																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
End of data!																									

Figure 7-42. IGMP Multicast Table window

VLAN Status

This table displays VLAN information for the specified VLAN.

VLAN Index: <input type="text" value="1"/> <input type="button" value="Search"/>																								
IEEE 802.1Q VLAN ID	Status	Creation time since switch power up																						
1	permanent	09:52:07																						
Current Egress Ports																								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Current Untagged Ports																								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Number of IEEE 802.1Q VLAN: 1																							<input type="button" value="Next"/>	
VLAN Status																								

Figure 7-43. VLAN Status window

The information is described as follows:

- **VLAN Index** – The VLAN for which the VLAN table is displayed.
- **Status** – This indicates the current status of the VID listed above.
- **Creation time since switch power up** – The hours, minutes, and seconds since the switch was last rebooted.

- **Current Egress Ports** – Displays the current egress ports on the VLAN.
- **Current Untagged Ports** – Displays the current untagged ports on the VLAN.

Maintenance

This category includes **TFTP Services (Update Firmware, Configuration File, Save Settings, and Save History Log)**, **Switch History**, **Ping Test**, **Save Changes**, **Factory Reset**, **Restart System**, **Connection Timeout**, and **Logout**.

TFTP Services

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

Please note that TFTP server software must be running on the management station for the TFTP services listed here to work.

Update Firmware



Update Firmware from Server	
Server IP Address	20 . 17 . 18 . 1
File Name	c:\temp\dgs3224.had
<input type="button" value="Start"/> <input type="button" value="Apply"/>	

Figure 7-44. Update Firmware from Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the switch. Click **Apply** to enter the server's IP address into the switch's RAM (use Save Changes to enter the address into the switch's non-volatile RAM). Click **Start** to initiate the file transfer.

The information is described as follows:

- **Server IP Address** – The IP address of the TFTP server.
- **File Name** – The full file name (including path) of the new firmware file on the TFTP server.

Configuration File

A configuration file can be downloaded from a TFTP server to the switch. This file is then used by the switch to configure itself.

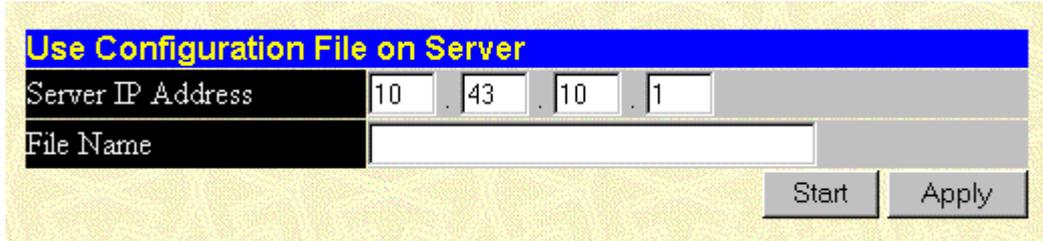


Figure 7-45. Use Configuration File on Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the switch. Click **Apply** to enter the server's IP address into the switch's RAM (use Save Changes to enter the address into the switch's non-volatile RAM). Click **Start** to initiate the file transfer.

The information is described as follows:

- **Server IP Address** – The IP address of the TFTP server.
- **File Name** – The full file name (including path) of the new firmware file on the TFTP server.

Save Settings

The switch's current settings can be uploaded to a TFTP Server by the switch's management agent.

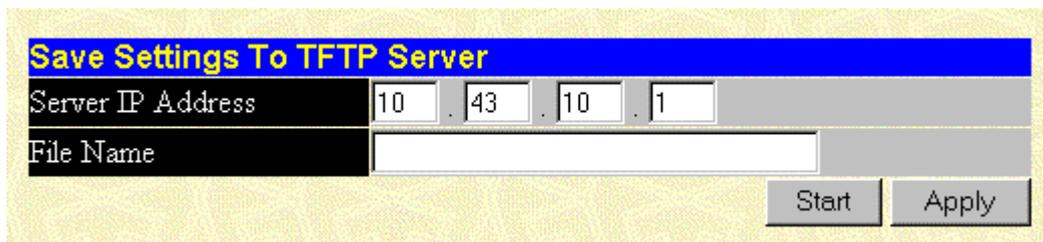


Figure 7-46. Save Settings To TFTP Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the switch. Click **Apply** to enter the server's IP address into the switch's RAM (use Save Changes to enter the address into the switch's non-volatile RAM). Click **Start** to initiate the file transfer.

Please note that if the user does not save configurations to NV-RAM, the configurations the user is uploading to a TFTP server will not be saved correctly.

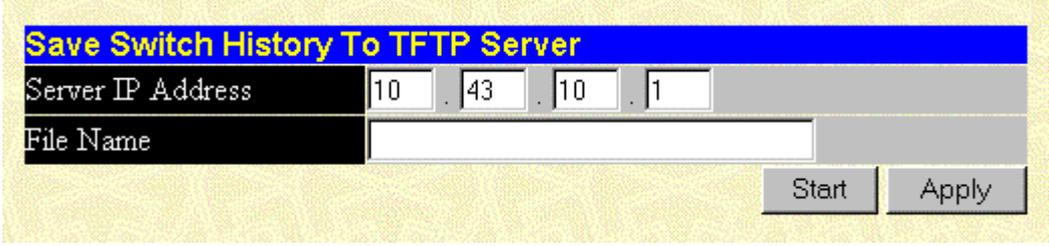
The information is described as follows:

- **Server IP Address** – The IP address of the TFTP server.
- **File Name** – The full file name (including path) of the new firmware file on the TFTP server.

Save History Log

The switch's management agent can upload its history log file to a TFTP server.

Please note that an empty history file on the TFTP server must exist on the server before the switch can upload its history file.



Save Switch History To TFTP Server					
Server IP Address	10	43	10	1	
File Name					
				Start	Apply

Figure 7-47. Save Switch History To TFTP Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the switch. Click **Apply** to enter the server's IP address into the switch's RAM (use Save Changes to enter the address into the switch's non-volatile RAM). Click **Start** to initiate the file transfer.

The information is described as follows:

- **Server IP Address** – The IP address of the TFTP server.
- **File Name** – The full file name (including path) of the new firmware file on the TFTP server.

Switch History

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

Switch History		
Sequence	Time	Log Text
224	000d06h26m	Successful login through web.
223	000d06h22m	Configuration saved to flash.
222	000d00h49m	Configuration saved to flash.
221	000d00h43m	Successful login through console.
220	000d00h43m	Successful logout through console.
219	000d00h27m	Configuration saved to flash.
218	000d00h26m	Successful login through console.
217	000d00h05m	Successful login through console.
216	000d00h00m	Module 1, Port 1 Link Up
215	000d00h00m	Module 1, Port 1 Link Down
214	000d00h00m	Module 1, Port 1 Link Up
213	000d00h00m	Cold Start
212	000d01h52m	Successful login through console.
211	000d00h00m	Successful login through console.
210	000d00h00m	Module 1, Port 6 Link Up
209	000d00h00m	Cold Start
208	000d00h03m	Upgrade firmware from successfully.
207	000d00h02m	Configuration saved to flash.
206	000d00h00m	Successful login through console.
205	000d00h00m	Module 1, Port 6 Link Up

Figure 7-48. Switch History window

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

The information is described as follows:

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

Ping Test

The switch is able to test the connection with another network device using Ping.

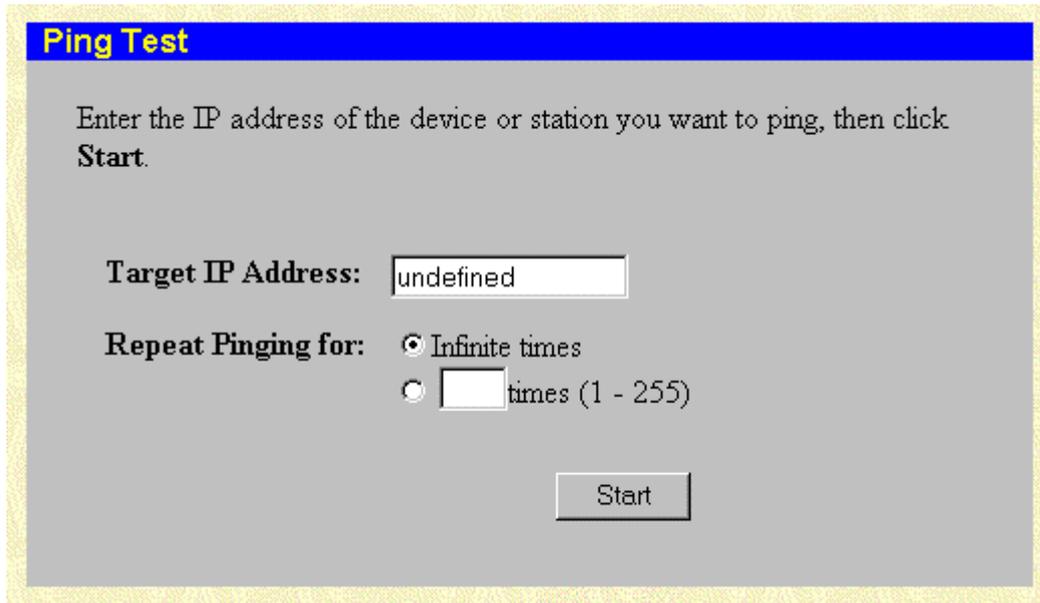


Figure 7-49. Ping Test window

Enter the IP address of the network device to be Pinged in the first field and select the number of test packets to be sent (3 is usually enough). Click **Start** to initiate the Ping program.

Save Changes

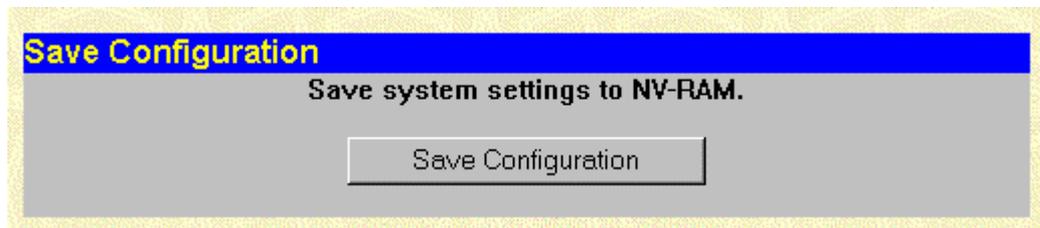


Figure 7-50. Save Configuration window

To save all the changes made in the current session to the switch's flash memory, click the **Save Configuration** button.

Factory Reset

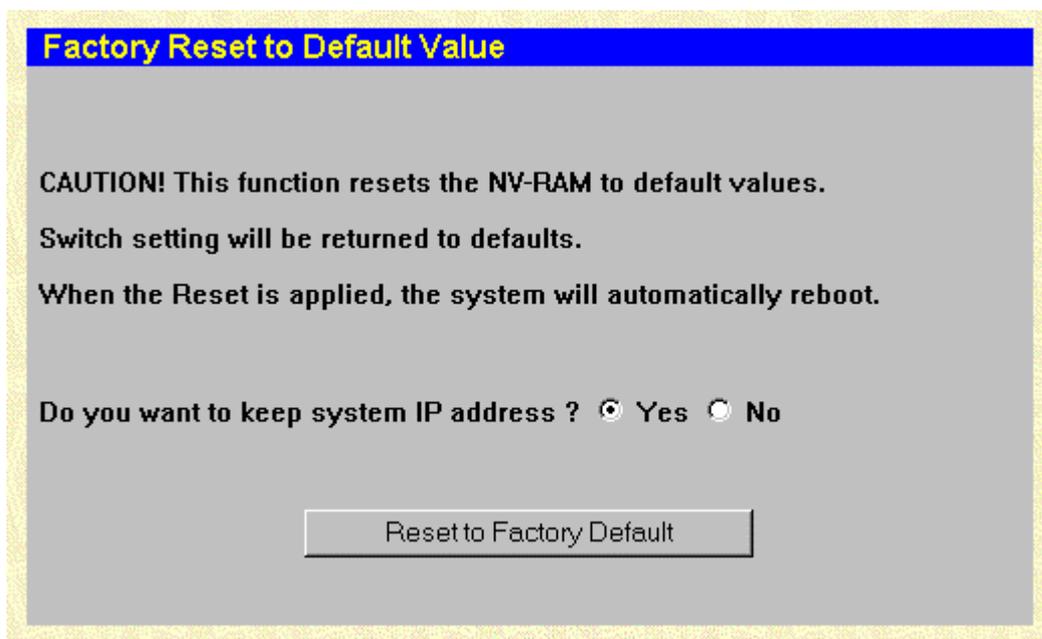


Figure 7-51. Factory Reset to Default Value window

A remote reset returns the switch to the initial parameters set at the factory. Click **Reset to Factory Default** to reset the switch.

Restart System

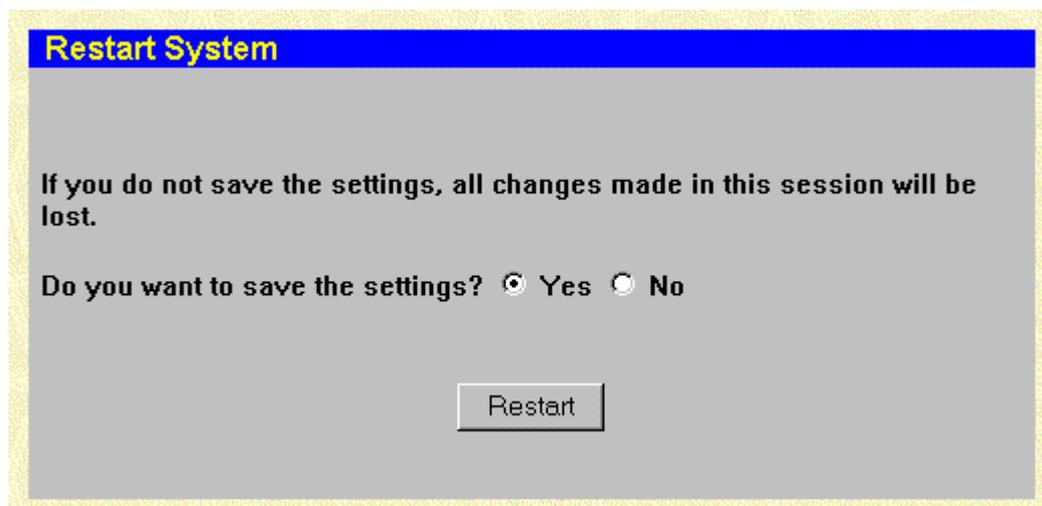


Figure 7-52. Restart System window

To perform a reboot of the switch, which resets the system, click the **Restart** button.

Connection Timeout

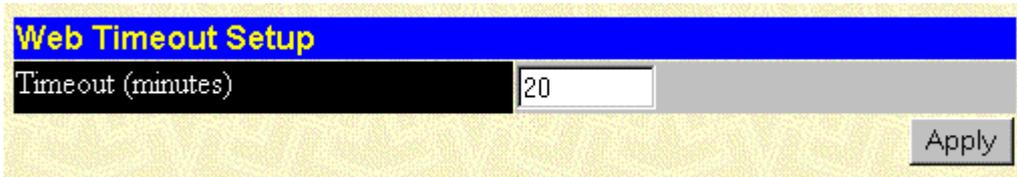


Figure 7-53. Web Timeout Setup window

To use this Web timeout feature, enter the desired age-out time and then click **Apply**.

Logout

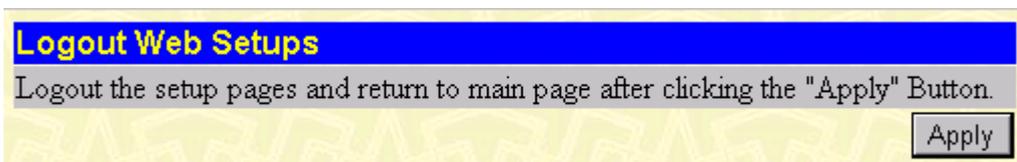


Figure 7-54. Logout Web Setups window

To exit the setup pages and return to the main page, click **Apply**.

Help

Click this button to access the online help files for the switch.

TECHNICAL SPECIFICATIONS

General			
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z Gigabit Ethernet IEEE 802.1Q Tagged VLAN IEEE 802.1P Tagged Packets IEEE 802.3ab 1000BASE-T IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 NWay auto-negotiation		
Protocols:	CSMA/CD		
Data Transfer Rates:	<table border="0"> <tr> <td>Half duplex</td> <td>Full duplex</td> </tr> </table>	Half duplex	Full duplex
Half duplex	Full duplex		
Ethernet:	<table border="0"> <tr> <td>10 Mbps</td> <td>20 Mbps</td> </tr> </table>	10 Mbps	20 Mbps
10 Mbps	20 Mbps		
Fast Ethernet:	<table border="0"> <tr> <td>100 Mbps</td> <td>200 Mbps</td> </tr> </table>	100 Mbps	200 Mbps
100 Mbps	200 Mbps		
Gigabit Ethernet:	2000 Mbps (Full duplex only)		
Topology:	Star		
Network Cables			
10BASE-T:	UTP Category 3, 4, 5 (100 meters max.) EIA/TIA- 568 100-ohm STP (100 meters max.)		
100BASE-TX:	UTP Cat. 5 (100 meters max.) EIA/TIA-568 100-ohm STP (100 meters max.)		
1000BASE-T:	UTP Cat. 5e (100 meters max.) UTP Cat. 5 (100 meters max.) EIA/TIA-568B 100-ohm STP (100 meters max.)		
GBIC:	50/125 μ m Multimode Fiber-optics (550 meters max.) 62.5/125 μ m Multimode Fiber-optics (550 meters max)		

	meters max.) 9µm Single-mode Fiber-optics (10 km max.)
Number of Ports:	20 10/100/1000 Mbps ports 4 GBIC ports

Physical and Environmental	
AC inputs:	100 – 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	79 watts maximum
DC fans:	4 built-in 50 x 50 x 15 mm fans
Operating Temperature:	0 to 50 degrees Celsius
Storage Temperature:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 388 mm x 66 mm (1U), 19 inch rack-mount width
Weight:	6 kg
EMI:	CE Mark Class A, C-Tick Class A, FCC Class A, BSMI Class A
Safety:	UL/CUL, TUV/GS

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	2 MB per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,100 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update. Supports 32K MAC address.
Priority Queues:	4 Priority Queues per port.
Forwarding Table Age Time:	Max age: 17–2100 seconds. Default = 300.

B***CABLE LENGTHS***

Use the following table to as a guide for the maximum cable lengths:

Standard	Media Type	Maximum Distance
GBIC	50/125 μ m Multimode Fiber	550 Meters
	62.5/125 μ m Multimode Fiber	550 Meters
	9 μ m Single-mode Fiber	5,000 Meters
1000BASE-T	Category 5e UTP Cable	100 Meters
	Category 5 UTP Cable (1000 Mbps)	
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100 Meters
10BASE-T	Category 3 UTP Cable (10 Mbps)	100 Meters

RUNTIME SWITCHING SOFTWARE DEFAULT SETTINGS

Load mode	Ethernet
Configuration update	Disable
Firmware update	Disable
Out-of-band baud rate	9600
RS232 mode	Console
IP address	10.90.90.90
Subnet mask	255.0.0.0
Default gateway	0.0.0.0
BootP service	Disable
TFTP server IP address	0.0.0.0
Auto log-out	10 min
User name	None
Password	None
MAC address aging time	300 secs
IGMP snooping	Disable
Switch GVRP	Disable
Telnet status	Enable
Web status	Enable
Device STP	Disable
Port STP	Enable
Port enable	Enable
Scheduling mechanism for COS queues	Strict
Trunk load sharing algorithm	Src address
Bridge max age	20 secs
Bridge hello time	2 secs
Bridge forward delay	15 secs
Bridge priority	32768
Port STP cost	19
Port STP priority	128
NWay	Enable
Flow control	Enable
Community string	"public", "private"
VLAN mode	IEEE 802.1Q
Management VLAN ID	1
Default port VID	1
Ingress rule checking	Disable



UNDERSTANDING AND TROUBLESHOOTING THE SPANNING TREE PROTOCOL

When the spanning-tree algorithm determines a port should be transitioned to the forwarding state, the following occurs:

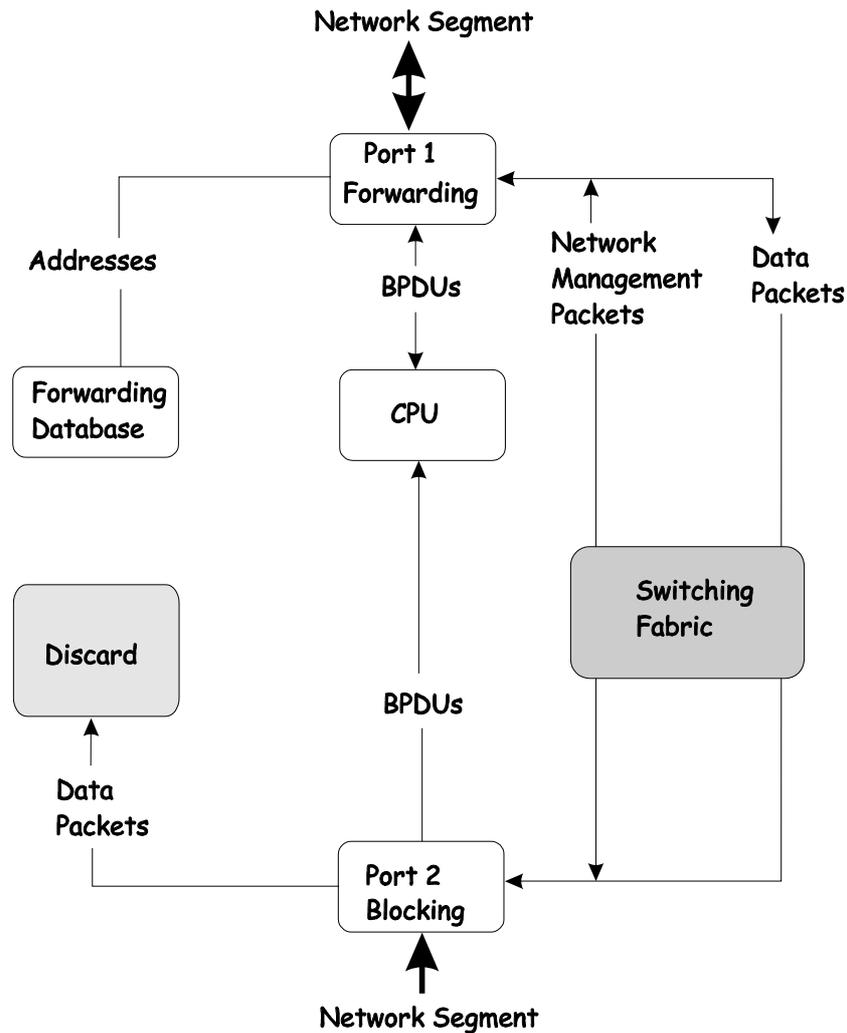
- The port is put into the listening state where it receives BPDUs and passes them to the switch's CPU. BPDU packets from the CPU are processed. If no BPDUs that suggest the port should go to the blocking state are received:
- The port waits for the expiration of the forward delay timer. It then moves to the learning state.
- In the learning state, the port learns station location information from the source address of packets and adds this information to its forwarding database.
- The expiration of forwarding delay timer moves the port to the forwarding state, where both learning and forwarding are enabled. At this point, packets are forwarded by the port.

Blocking State

A port in the blocking state does not forward packets. When the switch is booted, a BPDU is sent to each port in the switch putting these ports into the blocking state. A switch initially assumes it is the root, and then begins the exchange of BPDUs with other switches. This will determine which switch in the network is the best choice for the root switch. If there is only one switch on the network, no BPDU exchange occurs, the forward delay timer expires, and the ports move to the listening state. All STP enabled ports enter the blocking state following switch boot.

A port in the blocking state does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database
- Receives BPDUs and directs them to the CPU.
- Does not transmit BPDUs received from the CPU.
- Receives and responds to network management messages.



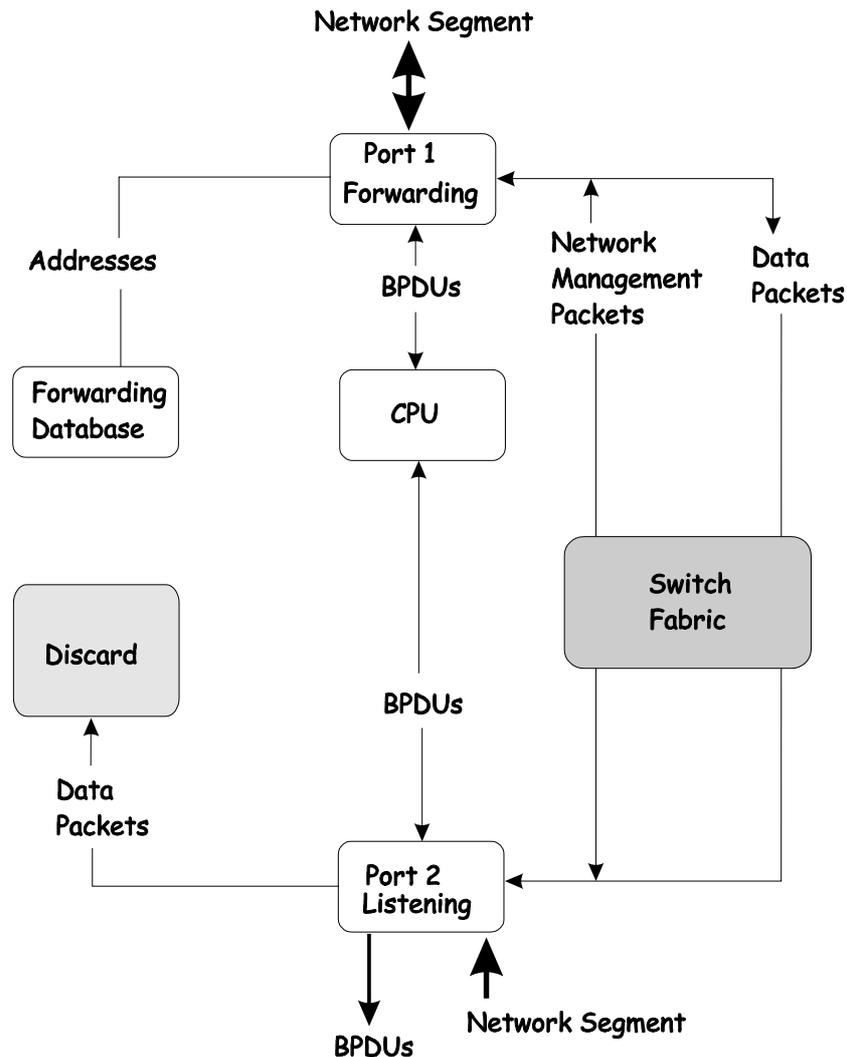
Listening State

The listening state is the first transition for a port from the blocking state. Listening is an opportunity for the switch to receive BPDUs that may tell the switch that the port should not continue to transition to the forwarding state, but should return to the blocking state (that is, a different port is a better choice).

There is no address learning or packet forwarding from a port in the listening state.

A port in the listening state does the following:

- Discards frames received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database
- Receives BPDUs and directs them to the CPU.
- Processes BPDUs received from the CPU.
- Receives and responds to network management messages.

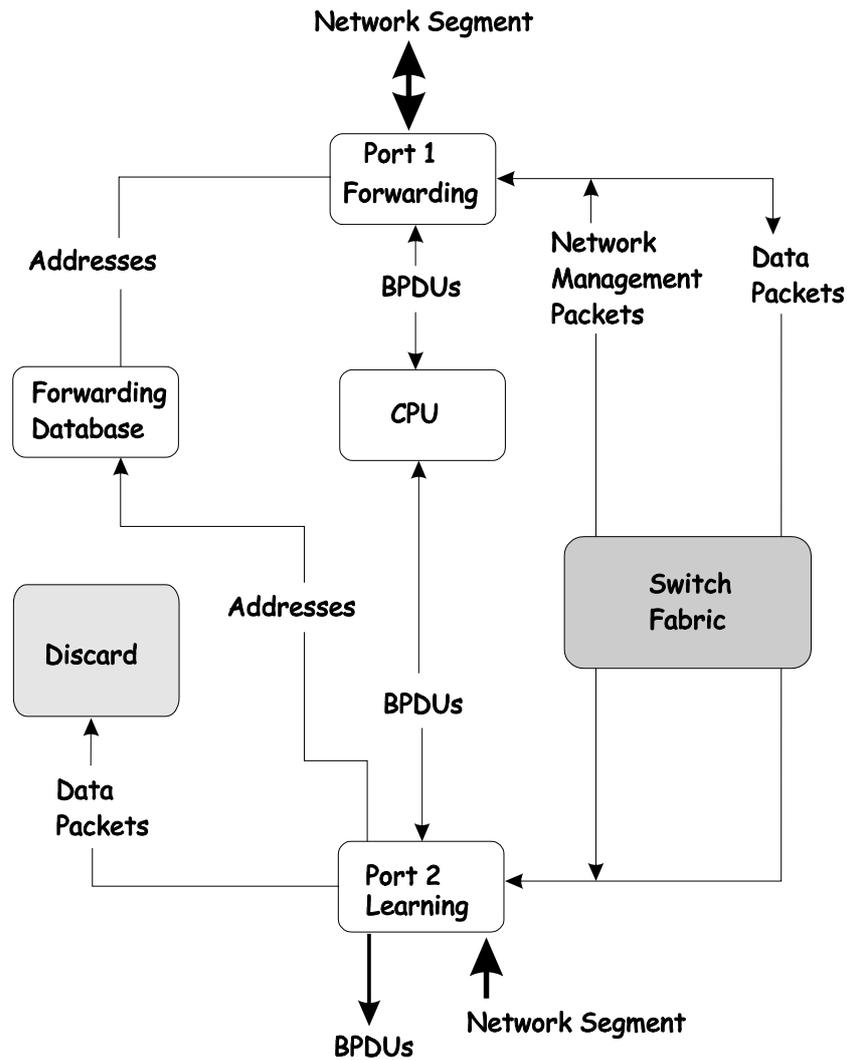


Learning State

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state.

A port in the learning state does the following:

- Discards frames received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Adds addresses to its forwarding database.
- Receives BPDUs and directs them to the CPU.
- Processes and transmits BPDUs received from the CPU.
- Receives and responds to network management messages.

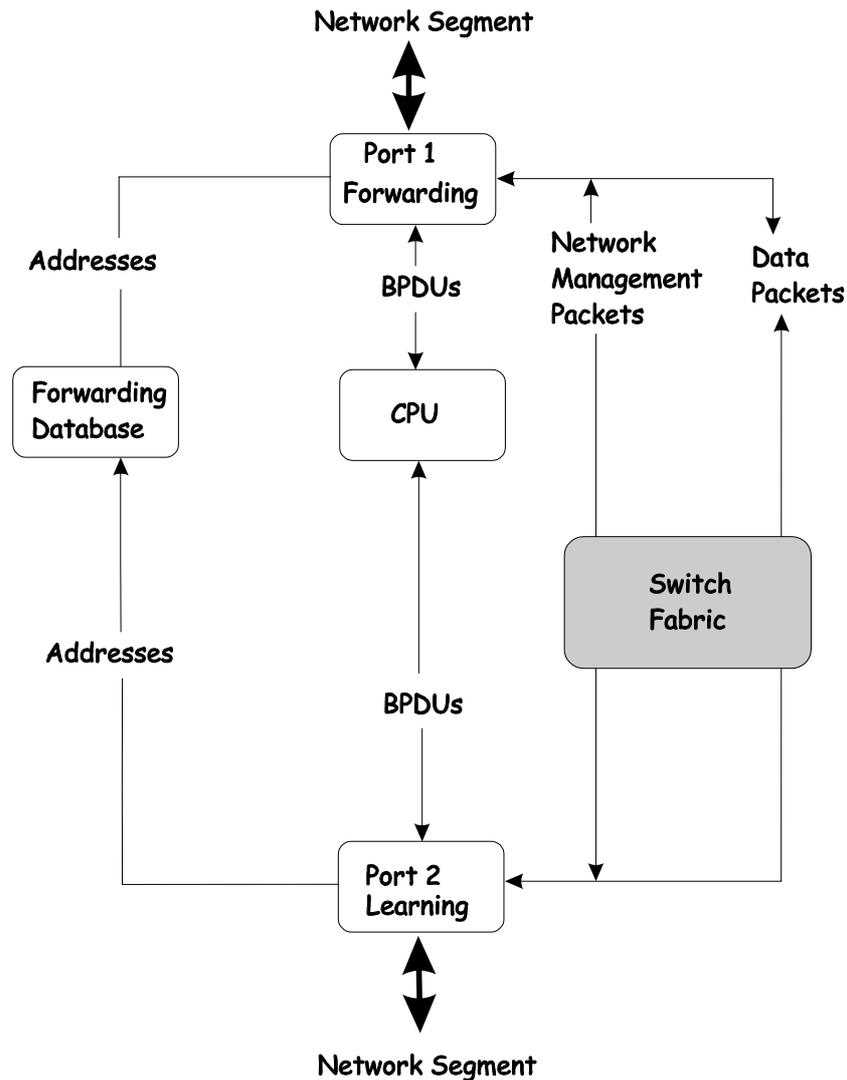


Forwarding State

A port in the forwarding state forwards packets. The port enters the forwarding state from the learning state when the forward delay timer expires.

A port in the forwarding state does the following:

- Forwards packets received from the network segment to which it is attached.
- Forwards packets sent from another port on the switch for forwarding.
- Incorporates station location information into its address database.
- Receives BPDUs and directs them to the system CPU.
- Receives and responds to network management messages.

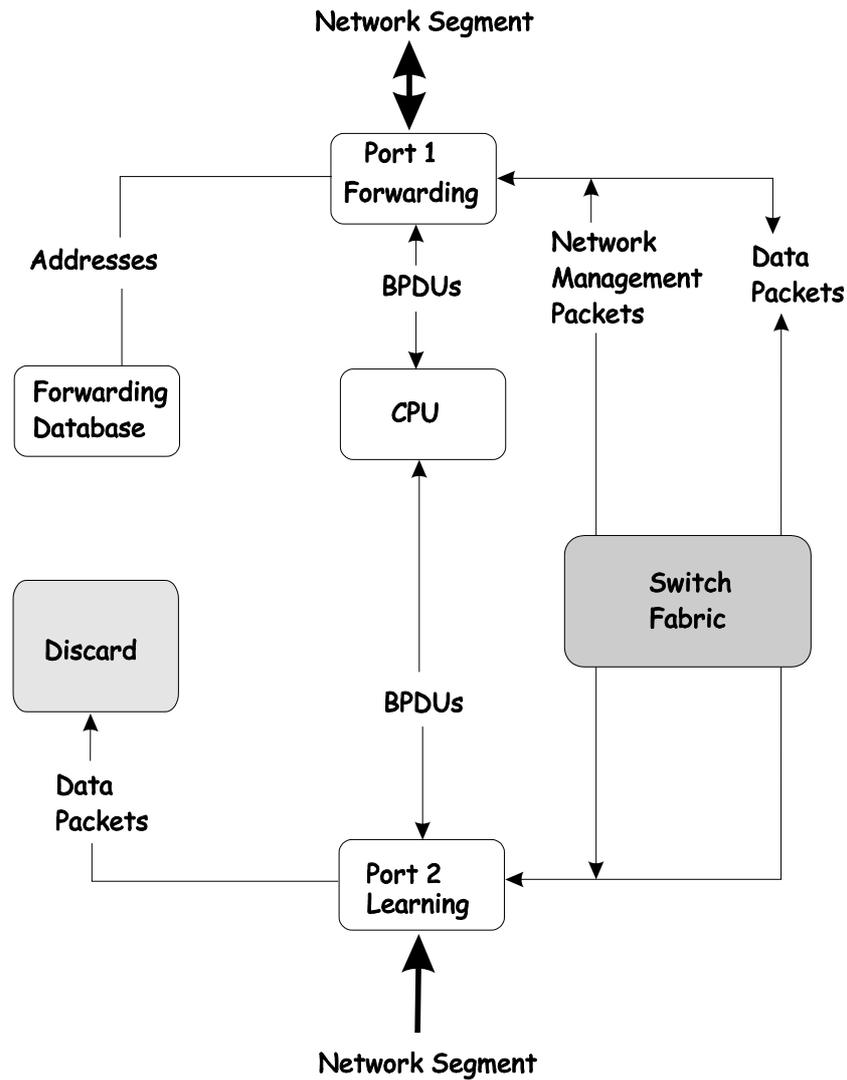


Disabled State

A port in the disabled state does not participate in frame forwarding or STP. A port in the disabled state is virtually non-operational.

A disabled port does the following:

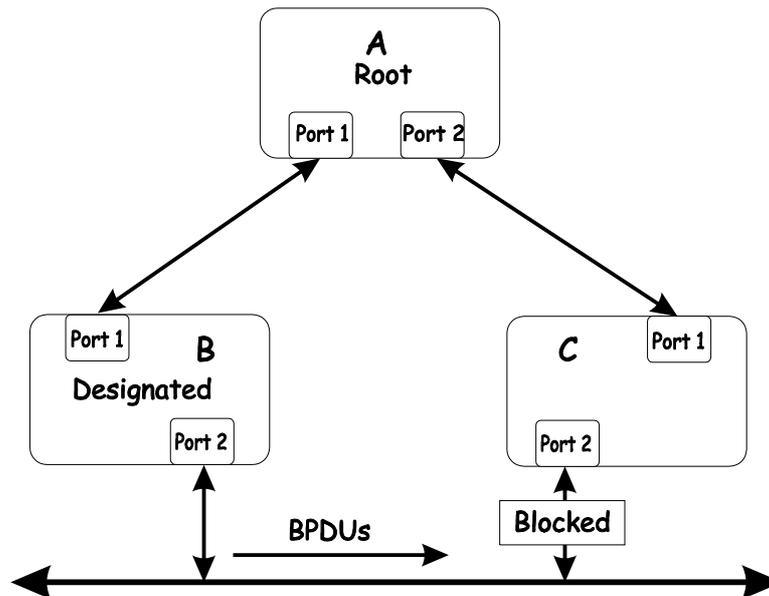
- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs, but does not direct them to the system CPU.
- Does not receive BPDUs for transmission from the system CPU.
- Receives and responds to network management messages.



Troubleshooting STP

Spanning Tree Protocol Failure

A failure in the STA generally leads to a bridging loop. A bridging loop in an STP environment comes from a port that should be in the blocking state, but is forwarding packets.



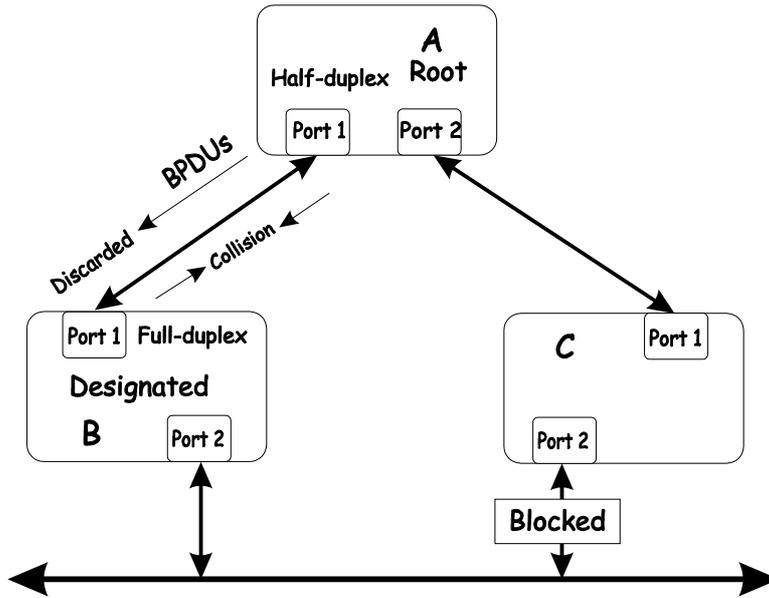
In this example, B has been elected as the designated bridge and port 2 on C is in the blocking state. The election of B as the designated bridge is determined by the exchange of BPDUs between B and C. B had a better BPDU than C. B continues sending BPDUs advertising its superiority over the other bridges on this LAN. Should C fail to receive these BPDUs for longer than the MAX AGE (default of 20 seconds), it could start to transition its port 2 from the blocking state to the forwarding state.

It should be noted: A port must continue to receive BPDUs advertising superior paths to remain in the blocking state.

There are a number of circumstances in which the STA can fail – mostly related to the loss of a large number of BPDUs. These situations will cause a port in the blocking state to transition to the forwarding state.

Full/Half Duplex Mismatch

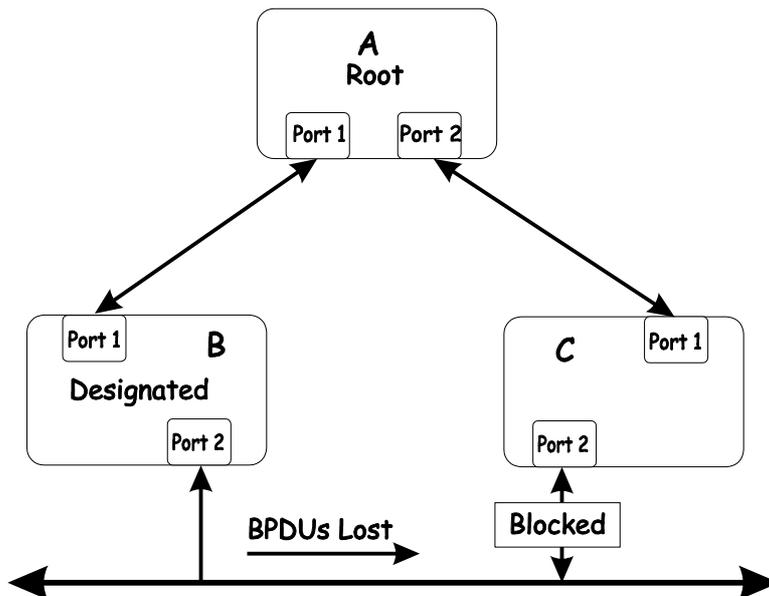
A mismatch in the duplex state of two ports is a very common configuration error for a point-to-point link. If one port is configured as a full duplex, and the other port is left in auto-negotiation mode, the second port will end up in half-duplex because ports configured as half- or full-duplex do not negotiate.



In the above example, port 1 on B is configured as a full-duplex port and port 1 on A is either configured as a half-duplex port, or left in auto-negotiation mode. Because port 1 on B is configured as a full-duplex port, it does not do the carrier sense when accessing the link. B will then start sending packets even if A is using the link. A will then detect collisions and begin to run the flow control algorithm. If there is enough traffic between B and A, all packets (including BPDUs) will be dropped. If the BPDUs sent from A to B are dropped for longer than the MAX AGE, B will lose its connection to the root (A) and will unblock its connection to C. This will lead to a data loop.

Unidirectional Link

Unidirectional links can be caused by an undetected failure in one side of a fiber cable, or a problem with a ports transceiver. Any failure that allows a link to remain up while providing one-way communication is very dangerous for STP.



In this example, port 2 on B can receive but not transmit packets. Port 2 on C should be in the blocking state, but since it can no longer receive BPDUs from port 2 on B, it will transition to the forwarding

state. If the failure exists at boot, STP will not converge and rebooting the bridges will have no effect. (Note: Rebooting would help temporarily in the previous example).

This type of failure is difficult to detect because the Link-state LEDs for Ethernet links rely on the transmit side of the cable to detect a link. If a unidirectional failure on a link is suspected, it is usually required to go to the console or other management software and look at the packets received and transmitted for the port. A unidirectional port will have many packets transmitted but none received, or vice versa, for example.

Packet Corruption

Packet corruption can lead to the same type of failure. If a link is experiencing a high rate of physical errors, a large number of consecutive BPDUs can be dropped and a port in the blocking state would transition to the forwarding state. The blocking port would have to have the BPDUs dropped for 50 seconds (at the default settings) and a single BPDU would reset the timer. If the MAX AGE is set too low, this time is reduced.

Resource Errors

The DGS-3224TG performs its switching and routing functions primarily in hardware, using specialized ASICs. STP is implemented in software and is thus reliant upon the speed of the CPU and other factors to converge. If the CPU is over-utilized, it is possible that BPDUs may not be sent in a timely fashion. STP is generally not very CPU intensive and is given priority over other processes, so this type of error is rare.

It can be seen that very low values for the MAX AGE and the FORWARD DELAY can result in an unstable spanning tree. The loss of BPDUs can lead to data loops. The diameter of the network can also cause problems. The default values for STP give a maximum network diameter of about seven. This means that two switches in the network cannot be more than seven hops apart. Part of this diameter restriction is the BPDU age field. As BPDUs are propagated from the root bridge to the leaves of the spanning tree, each bridge increments the age field. When this field is beyond the maximum age, the packet is discarded. For large diameter networks, STP convergence can be very slow.

Identifying a Data Loop

Broadcast storms have a very similar effect on the network to data loops, but broadcast storm controls in modern switches have (along with subnetting and other network practices) have been very effective in controlling broadcast storms. The best way to determine if a data loop exists is to capture traffic on a saturated link and check if similar packets are seen multiple times.

Generally, if all the users of a given domain are having trouble connecting to the network at the same time, a data loop can be suspected. The port utilization data in the switch's console will give unusually high values in this case.

The priority for most cases is to restore connectivity as soon as possible. The simplest remedy is to manually disable all of the ports that provide redundant links. Disabling ports one at a time, and then checking for a restoration of the user's connectivity will identify the link that is causing the problem, if time allows. Connectivity will be restored immediately after disabling a data loop.

Avoiding Trouble

Know where the root is located.

Although the STP can elect a root bridge, a well-designed network will have an identifiable root for each VLAN. Careful setup of the STP parameters will lead to the selection of this best switch as the root for each VLAN. Redundant links can then be built into the network. STP is well suited to maintaining connectivity in the event of a device failure or removal, but is poorly suited to designing networks.

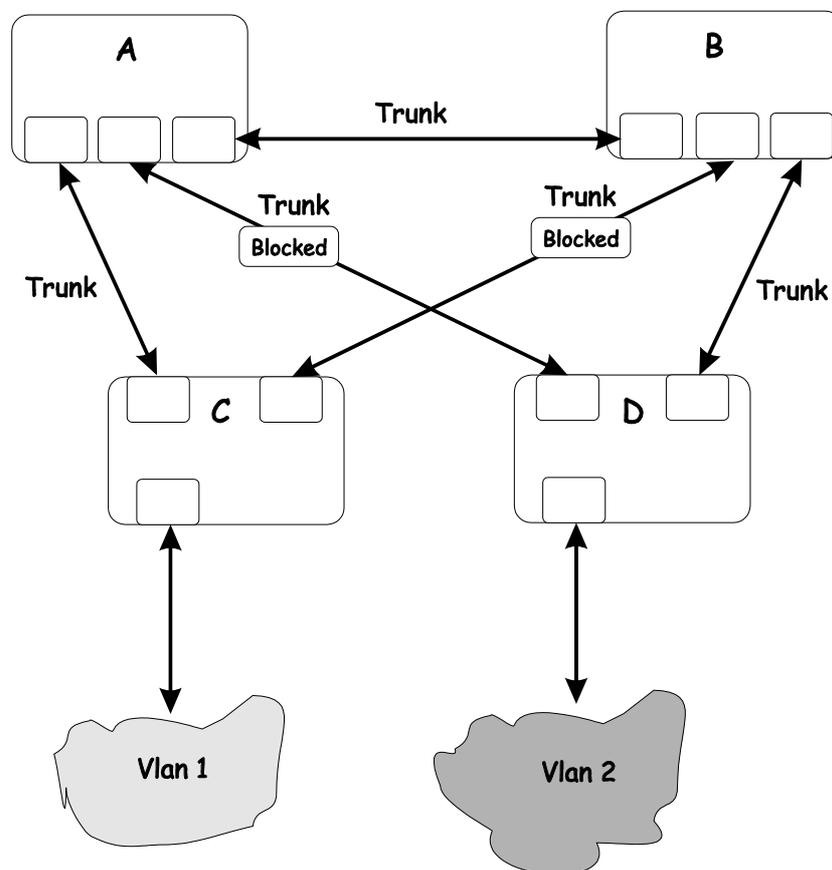
Know which links are redundant.

Organize the redundant links and tune the port cost parameter of STP to force those ports to be in the blocking state.

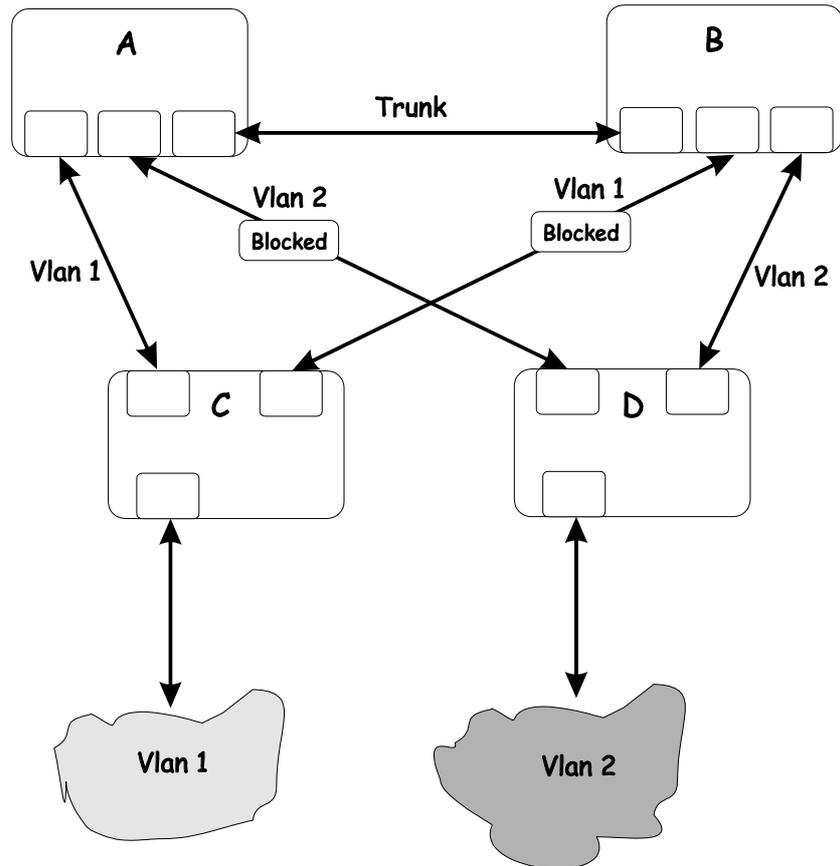
For each VLAN, know which ports should be blocking in a stable network. A network diagram that shows each physical loop in the network and which ports break which loops is extremely helpful.

Minimize the number of ports in the blocking state.

A single blocking port transitioning to the forwarding state at an inappropriate time can cause a large part of a network to fail. Limiting the number of blocked ports help to limit the risk of an inappropriate transition.



This is a common network design. The switches C and D have redundant links to the backbone switches A and B using trunks. Trunks, by default, carry all the VLAN traffic from VLAN 1 and VLAN 2. So switch C is not only receiving traffic for VLAN 1, but it is also receiving unnecessary broadcast and multicast traffic for VLAN 2. It is also blocking one port for VLAN 2. Thus, there are three redundant paths between switches A and B and two blocked ports per VLAN. This increases the chance of a data loop.



In this example, the VLAN definitions are extended to switches A and B. This gives only a single blocked port per VLAN and allows the removal of all redundant links by removing switch A or B from the network.



BRIEF REVIEW OF BITWISE LOGICAL OPERATIONS

AND

The logical AND operation compares 2 bits and if they are both "1", then the result is "1", otherwise, the result is "0".

	<i>0</i>	<i>1</i>
<i>0</i>	0	0
<i>1</i>	0	1

OR

The logical OR operation compares 2 bits and if either or both bits are "1", then the result is "1", otherwise, the result is "0".

	<i>0</i>	<i>1</i>
<i>0</i>	0	1
<i>1</i>	1	1

XOR

The logical XOR (*exclusive OR*) operation compares 2 bits and if exactly one of them is a "1", then the result is "1", otherwise the result is "0".

	<i>0</i>	<i>1</i>
<i>0</i>	0	1
<i>1</i>	1	0

NOT

The logical NOT operation simply changes the value of a single bit. If it is a "1", the result is "0", if it is a "0", the result is "1". This operation is carried out on a single bit.

<i>0</i>	<i>1</i>
<i>1</i>	<i>0</i>

INDEX

A	
AC inputs	125
AC power cord	4
Access Rights	
read only	68
read/write	68
Accessory pack	4
Administrator	30
Aging Time, definition of	15
Aging Time, range of	15
Automatic learning	16
B	
Baud Rate	60, 97
BOOTP protocol	39
BOOTP server	39
Bridge Forward Delay	20
Bridge Hello Time	20, 44
Bridge Max. Age	20, 44
Bridge Priority	20, 44
broadcast domains	22
C	
Changing the SNMP Manager Configuration	
parameters settings	68
Changing your Password	36
Community Name	13
Community name, definition of	67
Community names	
Private	68
Public	68
Connecting to the Switch	
VT100-compatible terminal	28
Connections	
Switch to End Node	9
Switch to Hub or Switch	9
console	8, 28, 29
console port	2, 7
Console port (RS-232 DCE)	11
Console port settings	11
Create/Modify User Accounts	36
D	
Data forwarding	2
Default Gateway	40
Diagnostic port	2
Dimensions	125
Dynamic filtering	16
E	
Egress port	22
F	
End Node	9
G	
factory reset	34
Filtering	15
Flash memory	3
Forwarding	15
Front Panel	7
H	
gateway router	13
I	
Humidity	125
J	
K	
L	
IEEE 802.1Q tagging	22
IEEE 802.1Q VLANs	23
Illustration of STA	20
Ingress port	22, 26
Internet Group Management Protocol (IGMP)	41, 83
IP address	12, 40, 68
IP Addresses and SNMP Community Names	12
IP Configuration	39
M	
LED Indicators	8
log in	36
Logging on	29
N	
O	
P	
Q	
R	
S	
T	
U	
V	
W	
X	
Y	
Z	
End Node	
factory reset	
Filtering	
Flash memory	
Forwarding	
Front Panel	
gateway router	
Humidity	
IEEE 802.1Q tagging	
IEEE 802.1Q VLANs	
Illustration of STA	
Ingress port	
Internet Group Management Protocol (IGMP)	
IP address	
IP Addresses and SNMP Community Names	
IP Configuration	
LED Indicators	
log in	
Logging on	
MAC Address Learning	
Main Menu	
Management	
Management Information Base (MIB)	
Max. Age	
MIB	
MIB objects	
MIB-II	
MIB-II (RFC 1213)	
MIBs	
mirror port	
Multicasting	
Network Classes	
Class A, B, C for Subnet Mask	
NV-RAM	
Operating Temperature	

P	
password	30
Port Mirroring	55
Port Priority	20, 45
ports	2
Power	8
Power Consumption	125
R	
RAM	33
RAM Buffer	125
Rear Panel	7, 8
refresh	29
RMON probe	55
RS-232	2
S	
Save Changes	29
Saving Changes	33
security	13, 23
Setup	4
sniffer	55
SNMP Community String	68
SNMP Manager Configuration	67
SNMP Manager Configuration parameter	
Status	68
SNMP Security (Community Names)	67
SNMP Trap Manager Configuration	67
Spanning Tree Algorithm	3
Spanning Tree Algorithm (STA)	16
Spanning Tree Protocol	16
Storage Temperature	125
Store and forward switching	2
subnet mask	40, 81
T	
tagging	22, 23
TCP/IP Settings	39
Telnet	28
terminal emulator	28
terminal parameters	28
Third-party vendors' SNMP software	14
Transmission Methods	125
Trap managers	13
Trap Type	
Authentication Failure	14
Cold Start	13
New Root	14
Topology Change	14
Traps	13
U	
unauthorized users	29
Unpacking	4
untagging	22, 23
User Accounts Management	36
username	30
V	
View/Delete User Accounts	37
VLAN	16, 22
VT100-compatible terminal	28
W	
Web-based management	77
Weight	125

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 (Australia): 1800-177100
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au
- Level 1, 434 St. Kilda Road, Melbourne, Victoria 3004 Australia
TEL: 61-3-9281-3232 FAX: 61-3-9281-3229 MOBILE: 0412-660-064
- Canada** **D-Link Canada**
2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5095 BBS: 1-965-279-8732
TOLL FREE: 1-800-354-6522 URL: www.dlink.ca
FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca
- Chile** **D-Link South America**
Isidora Goyechea 2934 of 702, Las Condes, Santiago, Chile, S. A.
TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: www.dlink.cl
E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl
- China** **D-Link China**
2F, Sigma Building, 49 Zhichun Road, Haidan District, 100080 Beijing, China
TEL: 86-10-88097777 FAX: 86-10-88096789 URL: www.dlink.com.cn
E-MAIL: liweii@digitalchina.com.cn
- Denmark** **D-Link Denmark**
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL: 45-43-969040 FAX: 45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk
- Egypt** **D-Link Middle East**
7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt
TEL: 20-2-635-6176 FAX: 20-2-635-6192 URL: www.dlink-me.com
E-MAIL: support@dlink-me.com & fateen@dlink-me.com
- Finland** **D-Link Finland**
Thlli-ja Pakkahuone Katajanokanlaituri 5, FIN- 00160 Helsinki
TEL: 358-9-622-91660 FAX: 358-9-622-91661 URL: www.dlink-fi.com
- France** **D-Link France**
Le Florilege #2, Allee de la Fresnerie, 78330 Fontenay le Fleury, France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr
E-MAIL: info@dlink-france.fr
- Germany** **D-Link Central Europe/D-Link Deutschland GmbH**
Schwalbacher Strasse 74, D-65760 Eschborn, Germany
TEL: 49-6196-77990 FAX: 49-6196-7799300 URL: www.dlink.de
BBS: 49-(0) 6192-971199 (analog) BBS: 49-(0) 6192-971198 (ISDN)
INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 E-MAIL: info@dlink.de
- India** **D-Link India**
Plot No.5, Kurla-Bandra Complex Rd., Off Cst Rd., 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 Mediterraneo Srl/D-Link Italia**
Via Nino Bonnet n. 6/b, 20154, Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it
- Japan** **D-Link Japan**
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp
E-MAIL: kida@d-link.co.jp

Netherlands **D-Link Benelux**
Fellenoord 1305611 ZB, Eindhoven, the Netherlands
TEL: 31-40-2668713 FAX: 31-40-2668666 URL: www.d-link-benelux.nl

Norway **D-Link Norway**
Waldemar Thranesgt. 77, 0175 Oslo, Norway
TEL: 47-22-991890 FAX: 47-22-207039

Russia **D-Link Russia**
Michurinski Prospekt 49, 117607 Moscow, Russia
TEL: 7-095-737-3389 & 7-095-737-3492 FAX: 7-095-737-3390 URL: www.dlink.ru
E-MAIL: vl@dlink.ru

Singapore **D-Link International**
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL: 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg
URL: www.dlink-intl.com

South Africa **D-Link South Africa**
102 – 106 Witchhazel Avenue, Einstein Park 2, Block B, Highveld Technopark,
Centurion, South Africa
TEL: 27 (0) 12-665-2165 FAX: 27 (0) 12-665-2186 URL: www.d-link.co.za
E-MAIL: attie@d-link.co.za

Spain **D-Link Iberia**
C/Sabino De Arana, 56 Bajos, 08028 Barcelona, Spain
TEL: 34 93 4090770 FAX: 34 93 4910795 URL: www.dlinkiberia.es
E-MAIL: info@dlinkiberia.es

Sweden **D-Link Sweden**
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-(0) 8-564-61900 FAX: 46-(0) 8-564-61901 E-MAIL: info@dlink.se
URL: www.dlink.se

Taiwan **D-Link Taiwan**
2F, No. 119 Pao-Chung Rd, Hsin-Tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 URL: www.dlinktw.com.tw
E-MAIL: dssqa@tsc.dlinktw.com.tw

Turkey **D-Link Middle East**
Deniz Bilgisayar, Buyukdere Cad. Naci Kasim Sk., No. 5 Mecidiyekoy, Istanbul, Turkey
TEL: 90-212-213-3400 FAX: 90-212-213-3420 E-MAIL: smorovati@dlink-me.com

U.A.E. **D-Link Middle East**
CHS Aptec (Dubai), P.O. Box 33550 Dubai U.A.E.
TEL: 971-4-366-885 FAX: 971-4-355-941 E-MAIL: Wxavier@dlink-me.com

U.K. **D-Link Europe**
4th Floor, Merit House, Edgware Road, Colindale, London NW9 5AB United Kingdom
TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 BBS: 44 (0) 181-235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. **D-Link U.S.A.**
53 Discovery Drive, Irvine, CA 92618, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033 BBS: 1-949-455-1779 & 1-949-455-9616
INFO: 1-800-326-1688 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®