DGS-3208F
Gigabit Ethernet Switch
User's Guide

First Edition (January 2000)
6DGS3208F.01
Printed In Taiwan

RECYCLABLE

Wichtige Sicherheitshinweise

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

WARRANTIES EXCLUSIVE

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

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

LIMITATION OF LIABILITY

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

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

Limited Warranty

Hardware:

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

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

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

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

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

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

Software:

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

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link

warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

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

D-Link Offices for Registration and Warranty Service

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

Trademarks

Copyright ©1999 D-Link Corporation.
Contents subject to change without prior notice.
D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

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

FCC Warning

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

CE Mark Warning

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

VCCI Warning

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

BSMI Warning

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

TABLE OF CONTENTS

ABOUT THIS GUIDE V

TERMS v
OVERVIEW OF THIS USER'S GUIDE v

INTRODUCTION 1

GIGABIT ETHERNET TECHNOLOGY 1
SWITCHING TECHNOLOGY 2
FEATURES 3
Ports 3
Performance features 3
Management 4

UNPACKING AND SETUP 5

UNPACKING 5
SETUP 6
DESKTOP OR SHELF INSTALLATION 6
RACK INSTALLATION 7
POWER ON 8
Power Failure 8

IDENTIFYING EXTERNAL COMPONENTS 9

FRONT PANEL 9
REAR PANEL 10
SIDE PANELS 11
LED INDICATORS 11

CONNECTING THE SWITCH 13

PC TO SWITCH 13
SWITCH TO SWITCH (OTHER DEVICES) 14

SWITCH MANAGEMENT 15

LOCAL CONSOLE MANAGEMENT.....15
Console port (RS-232 DCE).....16
IP Addresses and SNMP Community Names 16
Traps 17
MIBs 18
Packet Forwarding.....19
Aging Time 20
Spanning Tree Algorithm 20
STA Operation Levels.....21
User-Changeable Parameters.....23
Illustration of STA 24
Port Trunking 26
MAC-based Broadcast Domains 28

USING THE CONSOLE INTERFACE 30

CONNECTING TO THE SWITCH.....30
CONSOLE USAGE CONVENTIONS 31
FIRST TIME CONNECTING TO THE SWITCH.....32
Steps to Create Administrator or Normal User Access 33
Administrator and Normal User Privileges.....34
Save Configuration.....35
LOGIN ON THE SWITCH CONSOLE BY REGISTERED USERS 36
Add/Modify User Account 36
View/Delete User Account.....38
SETTING UP THE SWITCH 39
System Configuration 39
Configure IGMP Filtering.....60
Configure MAC-based Broadcast Domains.....62
Configure Trunk 68
Firmware and Configuration Update.....69
System Utilities.....71
SNMP Configuration.....74
SWITCH MONITORING.....76
Network Monitoring 76
RESETTING THE SWITCH 87
Restart System 88
Factory Reset to Default Value 88
Logout 89

WEB-BASED NETWORK MANAGEMENT 91

INTRODUCTION 91
GETTING STARTED 92
MANAGEMENT 92
Configuration 93
Bridge 106
Broadcast Domains 116
Trunk 120
Monitor 121
User 131
Utilities 132
Help 134

TECHNICAL SPECIFICATIONS 136

INDEX 139

ABOUT THIS GUIDE

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

Terms

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

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-3208F to your Gigabit Ethernet network.

- Chapter 5, *Switch Management*. 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-3208F.

1

INTRODUCTION

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

Gigabit Ethernet Technology

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

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

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

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

Switching Technology

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

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

The switch acts as a high-speed selective bridge between the individual segments. Traffic that needs to go from one segment to

another is automatically forwarded by the switch, without interfering with any other segments. This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

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

Features

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

Switch features include:

Ports

- Eight Gigabit Ethernet ports of fixed 1000BASE-SX multi-mode fiber interface.
- RS-232 DCE console port for diagnosing the Switch via a connection to a PC and console/out-of-band management.

Performance features

- Store and forward switching scheme capability to support rate adaptation and protocol conversion.

- Full duplex to allow two communicating stations to transmit and receive at the same time.
- Data forwarding rate 1,488,100 pps per port at 100% of wire-speed for 1000-Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 1,488,100 pps per port at 100% of wire-speed for 1000-Mbps speed.
- 12K active MAC address entry table per device with automatic learning and aging.
- 16 MB packet buffer per device.
- Supports broadcast storm rate filtering.

Management

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

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-3208F Gigabit Ethernet Switch
- Accessory pack: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This user's guide with Registration Card
- Diskette containing management software

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

Setup

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

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

Desktop or Shelf Installation

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

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

Rack Installation

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

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

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

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

Power on

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

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

- The Power LED indicator will light while the Switch loads onboard software, and should remain on as long as the switch has power.
- The Console LED indicator will remain *ON* if there is a connection at the RS-232 port, otherwise this LED indicator is *OFF*.

Power Failure

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

3

IDENTIFYING EXTERNAL COMPONENTS

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

Front Panel

The front panel of the Switch consists of 8 1000BASE-SX multi-mode fiber ports, an RS-232 communication port, and LED indicators.

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

- Eight Gigabit Ethernet ports of fixed 1000BASE-SX multi-mode fiber interface.
- RS-232 DCE console port for diagnosing the Switch via a connection to a PC and local console management.
- Comprehensive LED indicators that display the conditions of the Switch and status of the network. A description of these LED indicators follows (see *LED Indicators*).

Rear Panel

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

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

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

Side Panels

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

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

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

LED Indicators

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

Figure 3-4. The DGS-3208F Switch LED indicators

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

- **Console** This LED indicator is lit when the switch is being managed via out-of-band/local console management through the RS-232 console port using a straight-through serial cable. When a secured connection is established, this LED indicator is lit. Otherwise, it is *OFF*.

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

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

4

CONNECTING THE SWITCH

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

PC to Switch

A PC can be connected to the Switch via a fiber optic cable. The PC should be connected to any of the eight ports (1x - 8x) of the DGS-3208F.

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

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

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

- The Link/Act LED indicator lights up upon hookup.

Switch to Switch (other devices)

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

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

5

SWITCH MANAGEMENT

Local Console Management

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

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

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

The Spanning Tree Algorithm (STA) provides the capability for the Switch to operate properly with other Bridges in a SNMP network supporting the STA. Using the STA, the network will prevent

network loop, and automatically establish and activate a backup path in the event of a path failure.

Console port (RS-232 DCE)

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

The console port is set for the following configuration:

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

IP Addresses and SNMP Community Names

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

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

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

Traps

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

Traps are messages that alert you of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned *OFF* the Switch), or less serious like a port status change. The Switch generates traps and sends them to the network manager (trap managers). The following lists the types of events that can take place on the Switch.

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

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

The following are trap types a trap manager will receive:

- ♦ **Cold Start** This trap signifies that the Switch has been powered up and initialized such that software settings are

reconfigured and hardware systems are rebooted. A cold start is different from a factory reset.

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

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

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

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

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

MIBs

The information stored in the Switch is known as the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, MIB values inside the Switch can be retrieved from any SNMP-based network manager. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. These MIBs may also be retrieved

by specifying the MIB's Object-Identity (OID) at the network manager. MIB values can be either read-only or read-write.

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

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

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

Packet Forwarding

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

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

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

1. Permanent configuration of reserved addresses.
2. Explicit configuration of static filtering information.
3. Automatic learning of dynamic filtering information through observation of Switched Local Area Network traffic.
4. Aging out of filtering information that has been automatically learned.
5. Calculation and configuration of Switched Local Area Network topology.

Aging Time

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

The Aging Time can be from 1 to 99 minutes. A very long Aging Time can result with the out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions.

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

Spanning Tree Algorithm

The Spanning Tree Algorithm (STA) in the Switch allows you to create alternative paths (with multiple switches or other types of bridges) in your network. These backup paths are idle until the

Switch determines that a problem has developed in the primary paths. When a primary path is lost, the switch providing the alternative path will automatically go into service with no operator intervention. This automatic network reconfiguration provides maximum uptime to network users. The concept of the Spanning Tree Algorithm is a complicated and complex subject and must be fully researched and understood. Please read the following before making any changes.

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

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

STA Operation Levels

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

On the Bridge Level

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

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

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

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

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

On the Port Level

- **Root Port** Each switch has a Root Port. This is the port that has the lowest Path Cost to the Root Bridge. In case there are several such ports, then the one with the lowest Port Identifier is the Root Port.

- **Designated Port** This is the port on each Designated Bridge that is attached to the LAN segment for which the switch is the Designated Bridge.

- **Port Priority** The smaller this number, the higher the Port Priority is. With higher Port Priority, the higher the probability that the port will be selected as the Root Port.

- **Path Cost** This is a changeable parameter and may be modified according to the STA specification.

User-Changeable Parameters

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

- **Bridge Priority** A Bridge Priority can be from 0 to 65535. 0 is equal to the highest Bridge Priority.

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

- Note that the Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

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

- **Bridge Forward Delay** The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Observe the following formulas when you set the above parameters:

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

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

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

Illustration of STA

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

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

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

Figure 5-1. Before Applying the STA Rules

Figure 5-2. After Applying the STA Rules

STA parameters	Settings	Effects	Comment
Bridge Priority	lower the #, higher the priority	Increases chance of becoming the Root Bridge	Avoid, if the switch is used in workgroup level of a large network

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

Table 5-1. User-selective STA parameters

Port Trunking

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

The Switch supports up to four trunk groups, which may include from two to eight switch ports each.

Figure 5-3. Port trunking example

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

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

MAC-based Broadcast Domains

A MAC-based broadcast domain is a collection of users or ports grouped together for the purpose of secure, autonomous broadcasting and multicasting. Members of a MAC-based broadcast domain must all be directly connected to the Switch.

Creating MAC-based broadcast domains helps increase security and reduce overhead on the network. All packets entering such a domain will be forwarded only to the stations that are members of the domain. This includes even Multicast frames and unknown unicast frames.

MAC-based broadcast domains can also provide a level of security to your network. The Switch will only deliver packets between stations that are members of the domain.

The Switch supports up to 12 MAC-based broadcast domains, which are by their nature limited to the Switch itself and the devices connected to it. Two key features inherent in MAC-based broadcast domains are flexibility and security.

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

MAC-based broadcast domains include groups of individual devices. Communications can be restricted to only certain devices that are members of a common broadcast domain. This provides a high degree of security by allowing network managers to decide access rights on a per-device basis.

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

6

USING THE CONSOLE INTERFACE

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

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
- Arrow keys enabled

- 9,600 baud
- 8 data bits
- No parity
- One stop bit

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 a VT-100 compatible terminal mode) to access and control the Switch. All of the screens are for the most part 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 on or off using the space bar, excepting the entries on the Port Configuration screen .

2. Items in **[***square brackets***]** can be changed by typing in a new value. You can use the backspace and delete keys to erase characters behind and in front of the cursor.

3. The up and down arrow keys, the left and right arrow keys, the tab key and the backspace key, can be used to move between selected items. It is recommended that you use the ***tab key*** and ***backspace key*** for moving around console.

4. Items in UPPERCASE are commands. Moving the selection to a command and pressing Enter will execute that command, e.g. SAVE, EXIT, etc.

First Time Connecting To The Switch

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

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

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

Figure 6-1. Initial Screen, first time connecting to the Switch

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

Figure 6-2. Main Menu

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

Steps to Create Administrator or Normal User Access

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

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

2. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user

should have **Administrator** or **Normal User** privileges. (Use the space bar to toggle between the two options).

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

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

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

Administrator and Normal User Privileges.

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

The following table summarizes Administrator and Normal User privileges:

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

Menu	Administrator	Normal User
	Privilege	
Factory Reset	Yes	No
Restart System	Yes	No

Table 6-1. Administrator and Normal User Privileges

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

Save Configuration

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

Figure 6-3. Save Configuration screen

Login On The Switch Console By Registered Users

To log in once you have created a registered user,

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

Add/Modify User Account

To add or change your user password:

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

Figure 6-4. User Account Management menu

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

Figure 6-5. Add/Modify User Account screen

3. Type in your **Username** and press Enter.

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

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

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

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

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

View/Delete User Account

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

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

To view your user password:

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

Figure 6-6. View/Delete User Account screen

To delete your user password:

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

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

Setting Up The Switch

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

System Configuration

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

Figure 6-7. System Configuration menu

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

Configure IP Address

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

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

Figure 6-8. IP Configuration screen

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

- **BOOTP Service** Determines whether the Switch should 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 on a central BOOTP server; if this option is set the Switch will first look for a BOOTP server to provide it with this information before using the supplied settings.

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

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

- **Default Gateway** IP address that determines where frames with a destination outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an internetwork, or you do not want the Switch to be accessible outside your local network, you can leave this field blank.

Configure Console

You can use the **Console Configuration** screen to choose whether to use the Switch's RS-232C serial port for console management or

for out-of-band TCP/IP communications using SLIP, and to set the bit rate used for SLIP communications.

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

Figure 6-9. Console Configuration screen

The following fields can be set:

- Restart Setting:
- **Console Timeout** This setting for the restart of the console is *15 mins*, *30 mins*, *45 mins*, *60 mins*, or *Never*.
- **Serial Port** Determines whether the serial port should be used for out-of-band (SLIP) management or for console management, starting from the next time the Switch is restarted. In this field, you can toggle between *SLIP* or *Console* port type settings.

- **Baud Rate** Determines the serial port bit rate that will be used the next time the Switch is restarted. Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are 2400, 9600, 19,200 and 38,400 bits per second. The default setting in this Switch version is 9600.

Configure Switch

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

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

Figure 6-10. Switch Configuration screen

The fields you can set are:

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

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

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

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

Figure 6-11. Configure Advanced Switch Features screen

The field you can set is:

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

Configure Ports

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

To change the configuration of a port:

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

Figure 6-12. Port Configuration screen

2. Specify the port in the **Port (1-8)** field.

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

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

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

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

7. In the **Broadcast Storm Rising Action** and **Broadcast Storm Falling Action** fields, set the desired setting.

8. Press CTRL+S to let the changes take effect.

The **Speed/Duplex** field reflects the current condition of the port, *1000M/Full*. It is a read-only field and cannot be changed.

The fields you can set are:

- **Port (1-8)** Select the desired port in this field.
- **State** When you disable the state, the port will be partitioned from the rest of the network. In this partitioned state, it will only be able to accept management packets. All other packets will be dropped.
- **Flow Ctrl** Enables or disables IEEE 802.3x flow control on the port. Flow control allows the port to send a Pause packet to a transmitting IEEE 802.3x-compliant device, so that its buffers don't overflow and data is not lost.
- **Priority** Sets the priority for traffic arriving at this port to high, normal or low. Higher priority packets are processed first in the switch's packet queue.
- **Port Lock** When enabled, stops automatic learning for all stations connected to the port. Entries in the Forwarding Table for all devices connected to the port will age out. The only traffic this port will allow is traffic from machines whose MAC addresses are manually entered in the Static Forwarding Table.
- **Broadcast Storm** As a broadcast storm develops, the number of broadcast packets received on a port increases steadily. The Broadcast Storm controls make it possible to (1) prevent a broadcast storm from spreading from one port to others, and (2) restore normal forwarding of broadcast packets when the storm has abated.

  The **Rising Action** control and its associated **Threshold** control specify what action (if any) the Switch should take when broadcast traffic received on the port increases to or exceeds the equivalent of a specified number of broadcast

packets per second. The threshold can be set to 1 to 1,488,000 packets per second (the default is 500); the rising action can be set to *Do Nothing* (this is the default), *Blocking* (that is, discard all broadcast packets received on the port), or *Blocking-Trap* (discard all broadcast packets received on the port and send a trap to the trap manager[s]).

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

Configure Port Mirroring

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

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

Figure 6-13. Port Mirroring Configuration screen

To configure a mirror port, select the port from where you want to copy frames in the **Source Port** field. Then select the port which receives the copies from the source port in the **Target Port** field. The target port is where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe.

Configure Spanning Tree Protocol

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

To change the Protocol Parameters:

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

Figure 6-14. Spanning Tree Protocol Configuration menu

2. Choose **STP Parameters Setting** to access the following screen:

Figure 6-15. STP Parameters Setting screen

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

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

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

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

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

The information on the screen is described as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Bridge Priority(0-65535 Sec)** A Bridge Priority is a read-write object that can be set from 0 to 65535. This is the priority number of the bridge. The value is used in conjunction with the bridge MAC address to set the bridge

ID, which in turn is used when determining the root bridge of a multibridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. Zero is the highest priority.

To change the parameters on individual ports:

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

2. Choose **STP Custom Setting** from the **Spanning Tree Protocol Configuration** menu. The following screen appears:

Figure 6-16. STP Custom Setting screen

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

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

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

6. Press CTRL+S to apply the new settings.

Configure Filtering and Forwarding Table

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

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

Figure 6-17. Filtering and Forwarding Table Configuration screen

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

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

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

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

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

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

Figure 6-18. Custom Forwarding Table screen

- Under the **Destination MAC Address** heading a total of ten destination addresses will be seen per page. The Switch can hold up to 256 entries.

- Under the **Destination Port** heading a port number will be displayed for each corresponding destination address.

- Under the **Status** heading, the status will be displayed for each corresponding destination address. The status of the MAC address should show "in use".

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

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

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

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

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

Figure 6-19. Custom Filtering Table screen

To make a change to the **Custom Filtering Table**, choose *Add-Filter-Both* or *Remove* in the **Action** field. Then enter the **MAC Address** and press APPLY.

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

Figure 6-20. Custom Multicast Forwarding Table screen

To make a change to the Custom Multicast Forwarding Table, choose Add or Remove in the Action field. Then enter the MAC Address and the member port numbers in the desired fields. Press APPLY to put the changes into effect.

Configure IGMP Filtering

Internet Group Management Protocol (IGMP) allows multicasting on your network. When IP Multicast Filtering is enabled, the Switch can intelligently forward (rather that broadcast) IGMP queries and reports sent between devices connected to the Switch and an IGMP-enabled device hosting IGMP on your network. When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa.

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

Figure 6-21. IGMP Configuration screen

Items in this screen are defined as follows:

- **IP Multicast Filtering Age-out Timer (30-9999)** When this timer expires and the switch has not observed (snooped) any IGMP query packets asking whether any stations belong to any Multicast groups, the switch itself will send out queries and become the IGMP host on your network.

- **IP Multicast Filtering (IGMP Snooping)** This enables/disables the switch to intelligently forward IGMP and Multicast packets instead of broadcasting (flooding) them on all ports. This setting also enables IGMP Snooping, which enables the switch to read IGMP packets being forwarded through the switch in order to obtain forwarding

information from them (learn which ports contain Multicast members).

Configure MAC-based Broadcast Domains

If you are unsure of your knowledge of MAC-based broadcast domains, please review the section on MAC-based broadcast domains in the chapter of this manual entitled "Switch Management" before configuring the switch for such domains.

MAC-based Broadcast Domains Configuration screen #1 displays the current broadcast domain setting and allows you to specify the setting that will take effect the next time the Switch is restarted. The Restart Mode control can be set to "None" (this is the default setting) or to "MAC-based Broadcast Domains." This screen also lets you access MAC-based Broadcast Domains Configuration screen #2, through which you can access screens for adding and removing MAC-based broadcast domains and domain members.

To access MAC-based Broadcast Domains Configuration screen #1, choose Configure MAC-based Broadcast Domains from the System Configuration menu:

Figure 6-22. MAC-based Broadcast Domains Configuration screen #1

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

- **Current Mode** Displays whether MAC-based broadcast domains are currently enabled or disabled on the Switch.
- **Restart Mode** Choose from two settings for this mode: "None" or "MAC-based Broadcast Domains." After being restarted, the Switch will operate with MAC-based broadcast domains disabled or enabled, as specified here.

Configure MAC-Based Broadcast Domain

To set up a MAC-based broadcast domain, first choose Configure MAC-based Broadcast Domains from the System Configuration screen; then, from MAC-based Broadcast Domains Configuration screen #1, choose Configure MAC-based Broadcast Domains. MAC-based Broadcast Domains Configuration screen #2 will appear.

Figure 6-23. MAC-based Broadcast Domains Configuration screen #2

The commands in this screen let you create MAC-based broadcast domains (this is done by simply specifying names for them), remove them, and indicate (by specifying MAC addresses) which machines will be members of each such domain. Note that the Switch must be restarted for new settings to take effect.

Please note that if MAC-based broadcast domains are enabled, the Port Lock function is not supported in the Port Configuration screen and the Lock Address Table function located on the Configure Filtering and Forwarding table screen is not available.

Choose Add/Remove a MAC-Based Broadcast Domains to access the following screen:

Figure 6-24. Add/Remove MAC-based Broadcast Domains screen

The fields you can set are:

- **Action** Select the desired action by toggling between Add and Remove.
- **Domain Name** Enter the name or number of the MAC-based broadcast domain.

Press APPLY to create/remove the designated MAC-based broadcast domain.

The current MAC-based broadcast domain settings appear below the controls you can set. Broadcast Domains and Number of Members are read-only fields and cannot be directly changed.

To assign machines to a MAC-based broadcast domain, press Esc to return to MAC-based Broadcast Domains Configuration screen #2, then choose Add/Remove a MAC-based Broadcast Domain Member. The following screen will appear:

Figure 6-25. Add/Remove MAC-based Broadcast Domain Members screen #1

To place machines in a MAC-based broadcast domain or remove them from one, highlight the name of the desired broadcast domain and press ENTER. The following screen will appear:

Figure 6-26. Add/Remove MAC-based Broadcast Domain Members screen #2

The fields you can set are:

- **Action** Select the desired action by toggling between Add and Remove.
- **MAC Address** The MAC address of the domain member being added or removed.

Choose APPLY to have the selected action, Add or Remove, carried out. Please note that the Status field for each newly added MAC address will initially read Not-Apply. Your changes will take effect, and all Status fields will be updated, only after the settings are saved and the Switch is restarted with MAC-based broadcast domains enabled.

"Current Broadcast Domain," "Number of members," and (in the table below the controls you can set) "MAC Address" and "Status" reflect the current conditions. They are read-only fields and cannot be directly changed.

Configure Trunk

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

Figure 6-27. Port Trunking Configuration screen

The fields you can set are:

- **Index** Enter the index number (1 through 4, as shown in this screen) that you wish to give the new entry, or the index number of the entry that you wish to remove.

- **Active** Use the space bar to indicate whether you want to add or remove a trunk group. Be careful when removing trunk groups as the connections will return to normal operation, which may cause signal loops.

- **Description** Enter the desired group name. This can be any text string.
- **Port Member** Select two or more ports for this field. Use the arrow keys to move the cursor, and the V and hyphen keys to select and deselect ports.

Press APPLY to make the changes take effect. The new settings will appear in the table below the port trunking controls.

Firmware and Configuration Update

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

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

Figure 6-28. Firmware and Configuration Update screen

The fields you can set are:

- **Software Update Mode** Set to either *Network* or *SLIP*. Determines whether the configuration file should be obtained through the Ethernet network or through the console port.

- **TFTP Server Address** The IP address of the TFTP server where the configuration file is located. This entry is used only if the Firmware Update is set to *Enabled*. If BOOTP Service (see the **IP Configuration** screen under **Configure IP Address** on the **System Configuration** menu) is set to *Enabled*, the address will be obtained from the BOOTP server.

- **Firmware Update** Determines whether or not the Switch will try to look for a runtime image file over the network. If set to *Disabled*, none of the fields below have any effect.

- **File Name** The pathname of the runtime image file on your TFTP server to be downloaded.
- **Use Config File** Toggle to *Enabled* to download config file during reboot.
- **Config File Name** The name of the configuration file to be downloaded.

System Utilities

The **System Utilities** menu features **Ping Test**, **Upload Configuration Image File**, and **Upload Switch History File** commands.

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

Figure 6-29. System Utilities menu

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

Figure 6-30. Ping Test screen

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

The fields you can set are:

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

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

You can command the Switch to transmit a copy of its current configuration to any TFTP server on the network. This is done by choosing **Upload Configuration Image File** from the System Utilities screen. You will first be asked if you want to save the current configuration (including any recent, possibly unsaved

changes) to the Switch's non-volatile memory; then the following screen will appear:

Figure 6-31: Upload Configuration Image File screen

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

The System Utilities screen's **Upload Switch History File** function lets you command the Switch to send a record of operational events (see "Switch History" under "Switch Monitoring," further on in this chapter) to any TFTP server on the network. Choose this function to display the following screen:

Figure 6-32. Upload Switch History File screen

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

SNMP 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 detail list of Trap Types used for this Switch, see *Chapter 5, Switch Management, Traps* section.

SNMP (version 1) implements a rudimentary form of security by requiring that each request include a *community name*. A community name is an arbitrary string of characters used as a

"password" to control access to the Switch. If the Switch receives a request with a community name it does not recognize, it will trigger an authentication trap.

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

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

Figure 6-33. SNMP Configuration screen

The following parameters can be set:

- Community String/SNMP Community String Determines the community name to be included in the trap request.
- **Access Right** Allows each community to be separately set to either *Read Only* or *Read/Write*.

- **Status** Determines whether this community name entry is *Valid* or *Invalid*. An entry can be deleted by changing its status to *Invalid*.
- **IP Address** The IP address of the network management station to receive the trap.

Switch Monitoring

The Switch allows you to keep statistics on the operation of each port. The statistics obtained can be used to monitor the conditions and general efficiency of the Switch.

Network Monitoring

This display permits you to observe the condition of each individual port.

Traffic Statistics

To display the **Port Utilization** table:

1. Choose **Network Monitoring** from the main menu.
2. Choose **Traffic Statistics** from the **Network Monitoring** menu.
3. Choose **Port Utilization** from the **Traffic Statistics** menu.

Figure 6-34. Port Utilization screen

The information displayed above includes:

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

To display the **Port Traffic Statistics** table:

1. Choose **Network Monitoring** from the main menu.

2. Choose **Traffic Statistics** from the **Network Monitoring** menu.

3. Choose **Port Traffic Statistics** from the **Traffic Statistics** menu.

Figure 6-35. Port Traffic Statistics screen

The information displayed above includes:

- **Ports** This field always displays "*1 to 8*" in this 8-port Switch version.

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

- **Speed** The speed for each port is 1000M. When a link is up "1000M/Full" will be displayed. When a link is down "–" will be displayed.

- **% Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval.
- **Bytes Recv.** The number of good bytes received. This also includes local and dropped packets.
- **Bytes Sent** The number of good bytes sent from the respective port.
- **Frames Recv.** The number of good frames received. This also includes local and dropped packets.
- **Frames Sent** The number of good frames sent from the respective port.
- **Total Bytes Recv.** The number of bytes received, good and bad.
- **Total Frames Recv.** The number of frames received, good and bad.
- **Last Seen MAC** The MAC address of the device where the port information was most recently accessed.

To display the **Port Error Packet Statistics** table:

1. Choose **Network Monitoring** from the main menu.
2. Choose **Traffic Statistics** from the **Network Monitoring** menu.
3. Choose **Port Error Packet Statistics** from the **Traffic Statistics** menu.

Figure 6-36. Port Error Packet Statistics table

The information displayed above includes:

- **Ports** This field always displays "*1 to 8*" in this 8-port Switch version.
- **Update Interval** Select the desired update increment setting from: *1 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.
- **CRC Errors** The number of frames that fail the CRC integrity check.
- **Oversize Frames** The number of good frames with length greater than 1518 bytes and therefore are greater than the maximum legal length.
- **Fragments** The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

- **Jabbers** The number of frames with length more than 1518 bytes and with CRC error or misalignment (bad framing).
- **Late Collisions** The number of collisions that occur at or after the 64th byte (octet) in the frame.
- **Mac Rx Errors** The number of frames with received MAC Errors.
- **Dropped Frames** Counts received packets which are dropped due to any of the following reasons: lack of available receive buffers, port-disable, link-test-fail, spanning tree, or empty distribution list.
- **Total errors** The sum of the CRC Errors, Oversize Frames, Fragments, Jabbers, Late Collisions, Mac Rx Errors, and Dropped Frames counters.
- **Collisions** The number of collision errors.

To display the **Port Packet Analysis Statistics** table:

1. Choose **Network Monitoring** from the main menu.
2. Choose **Traffic Statistics** from the **Network Monitoring** menu.
3. Choose **Port Packet Analysis Statistics** from the **Traffic Statistics** menu.

Figure 6-37. Port Packet Analysis Statistics table

The information displayed above includes:

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

- **TX Octets** The number of good bytes sent from the respective port.
- **RX Octets** The number of good bytes received. This also includes local and dropped packets.
- **Total RX** The number of bytes received, good and bad.
- **Unicast RX/Unicast TX** The number of good unicast frames received and sent. This includes dropped unicast packets.
- **Multicast RX/Multicast TX** The number of good multicast frames received and sent. This includes local and dropped multicast packets.
- **Broadcast RX/Broadcast TX** The number of good broadcast frames received and sent. This includes dropped broadcast packets.

Forwarding Table

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

To display the **Forwarding Table**,

1. Choose **Network Monitoring** from the main menu.
2. Choose **Forwarding Table** from the **Network Monitoring** menu.

Figure 6-38. Forwarding Table

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

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

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

IGMP Status Information

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

To examine IGMP operation, choose Network Monitoring from the main menu and then choose IGMP Status Information. The IP Multicast Information screen will appear:

Figure 6-39. IP Multicast Information screen

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

The fields displayed are defined as follows:

- **IGMP Snooping** Indicates whether IGMP snooping is Enabled or Disabled.
- **Age-out Timer** Displays the time the Switch waits between IGMP queries.
- **Queries(TX)** The number of IGMP requests sent by the switch.

- **Queries(RX)** The number of IGMP requests that have arrived at a switch port.
- **Multicast Group** The Multicast IP address of the Multicast group being displayed.
- **MAC Address** The Multicast MAC address of the multicast group being displayed.
- **Reports** The number of notifications sent from each station to the IGMP host, signifying that the station is still (or wants to be) part of a multicast group.
- **Ports** The Switch ports supporting the selected multicast group.

Switch History

The Switch keeps a record of events that may be of interest to a network administrator: startups, reconfigurations, link activations and deactivations, firmware upgrades, and others. To view this record, choose Network Monitoring from the main menu, and then choose Switch History from the Network Monitoring menu. A screen similar to that shown below will appear:

Figure 6-40: Switch History screen

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

Resetting the Switch

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

Restart System

To perform a system reset, choose **Restart System** from the main menu. Please note there is no confirmation query before the system is rebooted.

Figure 6-41. Restart System screen

Factory Reset to Default Value

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

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

Figure 6-42. Factory Reset to Default Value screen

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

Logout

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

7

WEB-BASED NETWORK MANAGEMENT

Introduction

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

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

Getting Started

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

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

Management

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

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

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

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

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

All categories and options are explained below.

Configuration

This is the first category and is opened by default when you login to the Web-based management program. The **Configuration** options are listed below along with explanations for each one.

Basic Setup

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

The remaining information in the screen includes:

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

- **Hardware Revision** Version number of the Switch's hardware.

TCP/IP Setup

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

The information is described as follows:

- **IP Address** The Internet address for the device.
- **Subnet Mask** The subnet mask determines the level of the subnet that the Switch is on.
- **Default Gateway** The default router for the device.

- **Send Bootp Request Upon Power Up** Toggle between *Enable* and *Disable* to determine whether the IP address, subnet mask, and default gateway settings are automatically assigned by the BOOTP server or manually.

Advanced

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

Ports Setup

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

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

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

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

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

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

6. Specify settings for the broadcast storm controls.

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

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

7. Click Apply to let your changes take effect.

Port Mirror

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

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

Trap Manager

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

The information is described as follows:

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

SNMP Manager

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

The information is described as follows:

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

Download

Firmware and configuration updating can be done from the screen above.

The information is described as follows:

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

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

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

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

- **Use Config File** Determines whether or not the Switch should download its configuration file the next time it is booted.
- **Config File Name** The path and configuration name on the TFTP server.
- **Last TFTP Server Address** The IP address of the TFTP server where the configuration file was located in the last configuration change.

Console

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

The default serial port settings are:

Baud Rate=9600

Data Bits=8

Flow Control=XON/XOFF

Parity=None

Stop Bits=1

The information is described as follows:

- **Console Timeout** Choose *Never*, *15 minutes*, *30 minutes*, *45 minutes*, or *60 minutes* for the desired refresh setting.

- **Serial Port** The options for the current console port setting are *Console* or *Slip*.

- **Baud Rate** Determines the serial port bit rate that will be used the next time the Switch is restarted. Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are 2400, 9600, 19,200 and 38,400 bits per second. The default setting in this Switch version is 9600.

Save

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

Reset

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

Bridge

This is the second category of the Web-based management program. The **Bridge** options are listed below along with explanations for each one.

Switch STP

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" chapter for a detailed explanation.

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

The information on the screen is described as follows:

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

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

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

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

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

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

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

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

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

- **Root Priority(Sec)** Read-only object displays the priority number of the root bridge of the Spanning Tree. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multibridged network. The root bridge is responsible for processing data packets

when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. A bridge priority ranges from 0 to 65535, with 0 being the highest priority.

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

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

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

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

bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. Zero is the highest priority.

Port STP

The information on the screen is described as follows:

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

becoming the root port. Port priority ranges from 0 to 255, with 0 being the highest port priority.

Address Setup

The **Bridge** command group's **Address Setup** command lets you stop or restart MAC address learning, adjust address table size, and control how long learned addresses are retained in the table. Choosing Address Setup displays the following screen:

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

- **Address Table Lookup Mode** This setting allows the user to tailor the MAC address look up procedure. Choices are Level 0, Level 1, Level 2, Level 3, Level 4, Level 5, Level, 6, Level 7. The

higher the level, the more MAC addresses can be learned by the Switch. However, a side effect is that throughput will be degraded the higher the level you select. This setting will take effect after your system reboots.

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

FDB Table

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

Custom FDB

To use the MAC forwarding function, enter the MAC address of the device to which the specified port permanently forwards traffic in the **Destination Address** field and enter the port number that permanently forwards traffic from the specified device in the **Destination Port** field. Then click Apply.

The information in the screen is described as follows:

- **Destination Address** The MAC address of the device to which the specified port permanently forwards traffic.

- **Destination Port** The port number that permanently forwards traffic from the specified device, regardless of the device's network activity or current network congestion.

Filter Table

MAC filtering allows the Switch to block inbound traffic from unknown or unwanted devices by mapping a port to a source MAC address.

To use the MAC filtering function, enter the MAC address of the device allowed to send traffic in the **MAC Address** field and select the desired setting in the **Filter Status** field. Then click Apply.

The information in the screen is described as follows:

- **MAC Address** The Ethernet address of the MAC filtering table entry.
- **Filter Status** One filter status option is available, *Source/Destination*.

Multicast FDB (Custom Multicast Forwarding Table)

The Custom Multicast Forwarding Table screen allows you to forward traffic over each port for one multicast group. To access this screen, select Multicast FDB from the Bridge group. The following screen will appear:

To make a change to the Custom Multicast Forwarding Table, enter a MAC address, select a port number, and click Apply. Entries can be removed using the table in the bottom half of the screen.

IGMP Setup

The Bridge command group's **IGMP Setup** command lets you check and adjust Internet Group Management Protocol settings, which affect handling of IP multicast packets. Choosing IGMP Setup from the Bridge group displays the following screen:

- **IP Multicast Filtering Age-out Time** When this amount of time (in seconds) expires and the Switch has not observed (snooped) any IGMP query packets asking whether any stations belong to any multicast groups, the Switch itself will send out queries and become the IGMP host on your network. To change the setting, click in the box and type a figure from 30 to 9999.

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

Broadcast Domains

A MAC-based broadcast domain is a collection of users or ports grouped together for the purpose of secure, autonomous broadcasting and multicasting. Members of a MAC-based

broadcast domain must all be directly connected to the Switch. The Switch supports up to twelve MAC-based broadcast domains.

The Broadcast Domains command group contains two functions: Mode Setup and MAC-based.

Mode Setup

Choosing Mode Setup from the Broadcast Domains group displays the following screen:

In this screen, **Current Mode** is the current setting of the Switch's broadcast domains function. This can be either **None** (no broadcast domains) or **MAC-based** (that is, support for MAC-based broadcast domains enabled). The **Restart Mode** control lets you specify the setting that is to take effect the next time the Switch is restarted. Remember that you must click **Apply** *and* restart the Switch to make your selection the current mode.

Mac-based

Choosing **Mac-based** from the Broadcast Domains group displays the following screen:

This screen lets you create and remove MAC-based broadcast domains. In the **Domain Name** field, which is initially blank, type the name or number that you wish to give the domain; then click Apply to add the name to the table. The screen will change as shown below:

You can then click the button under **Remove** to remove the domain, or the arrow under **Enter** to add entries to it. Clicking the arrow under **Enter** displays the following screen:

This screen lets you designate particular machines on your network as members of the MAC-based broadcast domain named in the title above the settings area. To add a machine to the domain, click in the **MAC Address** field, type the machine's MAC address, and click **Apply**. The address will appear in the table in the lower part of the screen. You can then view its status (which depends on whether the setting has been saved and the Switch restarted) or, if you wish, remove it by clicking the button under **Remove**.

Trunk

Port trunking is used to combine a number of ports together to make a single high-bandwidth data pipeline. The participating parts are called members of a trunk group. The Switch supports up to four trunk groups, which may include from two to eight Switch ports each.

To check or change port trunking settings, click the "expand" box next to **Trunk** and choose **Port Trunking**. The screen shown below will appear:

To create a trunk group, click in a box in the **Description** column and type a name or number; then check the boxes for two or more ports (making sure none is used by any other trunk group), select the status you want (Enabled or Disabled), and click **Apply**.

Monitor

This is the fifth category of the Web-based management program. The **Monitor** options are listed below along with explanations for each one.

Overview

The information on the Switch Statistics table is described as follows:

- **TX frames/sec** Counts the total number of frames transmitted from a selected port per second since the Switch was last rebooted.
- **RX frames/sec** Counts all valid frames received on the port per second since the Switch was last rebooted.
- **% of Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval.

Traffic

The port statistics shown by default are those for the port you last configured. Once in the Port Statistics screens, you can click any port on the switch graphic to show statistics for that port.

The information is described as follows:

- **Link Status** Indicates whether the port is online and working (*1000/Full/Flow control off* or *1000/Full/Flow control on*) or not (*Link Down*).

- **Utilization** Current utilization for the port, as a percentage of total available bandwidth.

- **Last Screen MAC** The MAC address of the most recent screen.

Traffic in Bytes:

- **Bytes Sent** Counts the number of bytes successfully sent from the port.

- **Bytes Received** Counts the total number of bytes (octets) included in valid (readable) frames.
- **Total Bytes Received** Counts the total number of bytes received on the port, whether in valid or invalid frames.

Traffic in Frames:

- **Frames Sent** Counts the total number of frames transmitted from the port.
- **Frames Received** Counts all valid frames received on the port.
- **Total Frames Received** Counts the number of frames received on the port, whether they were valid or not.

Utilization

The information is described as follows:

- **Last Detected Source Address** MAC address of the last source accessed.

Errors

The information is described as follows:

- **Link Status** Indicates whether the port is online and working (*1000/Full/Flow control off* or *1000/Full/Flow control on*) or not (*Link Down*)..

- **Jabber** Counts frames longer than the maximum 1518 bytes (octets) with either bad framing or an invalid CRC.

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

Other errors:

- **CRC + Alignment** Counts otherwise valid frames that did not end on a byte (octet) boundary.
- **Late Collision** Counts collisions that occur at or after the 64th byte (octet) in the frame. This may indicate that delays on your Ethernet are too long, and you have either exceeded the repeater count or cable length specified in the Ethernet standard.
- **MAC Received Error** Counts bit patterns with illegal encodings. This may indicate noise on the line.
- **Oversize Frames** Counts packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Received Bad Fragments** The number of good frames with length less than the 64-byte (octet) minimum defined by the Ethernet standard. These are usually caused by collisions.
- **Total Errors** The sum of the CRC + Alignment, Late Collision, MAC Received Error, Oversize Frames, and Received Bad Fragments counters.
- **Collisions** The best estimate of the total number of collisions on this Ethernet segment.

Analysis

The information is described as follows:

- **Update Interval** The polling time interval can be set from 5 to 60 seconds, in 5 second increments. Click the Submit button once the update interval has been selected.

- **64** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

- **65-127** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

- **128–255** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

- **256-511** The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
- **512-1023** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
- **1024-1518** The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
- **RX (good)** The number of good frames received. This also includes local and dropped packets.
- **TX (good)** The number of good frames sent from the respective port.
- **Total RX** The number of frames received, good and bad.
- **TX Bytes** The number of good bytes sent from the respective port.
- **RX Bytes** The number of good bytes received. This also includes local and dropped packets.
- **Total RX** The number of bytes received, good and bad.
- **Unicast** The total number of good packets that were directed to a unicast address. Note that this does not include dropped unicast packets
- **Multicast** The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address

- **Broadcast** The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

IGMP Status

The Monitor group's IGMP Status command lets you examine the operation of the Internet Group Management Protocol (IGMP). The Switch can recognize IGMP queries and reports sent between stations and an IGMP router. When enabled for IGMP snooping, the Switch can open or close a port to specific devices based on the IGMP messages sent from the device to the router or vice versa.

To examine IGMP operation, choose IGMP Status from the Monitor group. The following screen will appear:

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

The fields displayed are defined as follows:

- **Snooping** Indicates whether IGMP snooping is Enabled or Disabled.
- **Age-out Timer** Displays the time the Switch waits between IGMP queries.
- **Queries(TX)** The number of IGMP requests sent by the switch.
- **Queries(RX)** The number of IGMP requests that have arrived at a switch port.

Click the **Refresh** button on the right to update the display with the latest information from the Switch. A second table in the lower part of the screen shows the following information:

- **Multicast Group** The Multicast IP address of the Multicast group being displayed.
- **MAC Address** The Multicast MAC address of the multicast group being displayed.
- **Reports** The number of notifications sent from each station to the IGMP host, signifying that the station is still (or wants to be) part of a multicast group.
- **Ports** The Switch ports supporting the selected multicast group.

History Log

The Switch keeps a record of events that may be of interest to a network administrator: startups, reconfigurations, link activations and deactivations, firmware upgrades, and others. To view this record, choose History Log from the Monitor command group. A screen similar to that shown below will appear:

The Switch can be commanded to upload its history via TFTP to a machine you specify. See the description of the Utilities group's Upload History command, further on in this chapter.

User

This is the sixth category of the Web-based management program. The **User** option is listed below along with an explanation.

To add or change a User Account, fill in the appropriate information in the **User Name**, **Old Password**, **New Password**, and **Confirm New Password** fields. Then select *General User* or *Administrator* in the **Access Level** control and click Apply.

To delete a User Account, click the "X" icon in the delete column on the User Account Table at the bottom of the screen.

Utilities

The Utilities command group contains two commands, Upload Image and Upload History. "Upload" here means "send from the Switch to the specified TFTP server."

Upload Image

The Upload Image function lets you retrieve the Switch's current configuration and save it for later use in configuring this or an identical switch. For information on using an uploaded

configuration image file, see the description of the Configuration group's Download command earlier in this chapter.

Choosing Upload Image from the Utilities group displays the following screen:

To have an image of the Switch's current configuration uploaded to a TFTP server on your network, enter the server's IP address, supply a valid file name, and click Apply.

Upload History

The Switch keeps a record of events that may be of interest to a network administrator: startups, reconfigurations, link activations and deactivations, firmware upgrades, and others. You can view this record by choosing History Log from the Monitor command group. You can also upload it from the Switch using the Utilities group's Upload History function. When you choose Upload History, the following screen appears:

To have a record of recent operational events uploaded to a TFTP server on your network, enter the server's IP address, supply a valid file name, and click Apply.

Help

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

Netscape
File Edit View Go Communicator Help
DGS-3208
Gigabit Switch
Power Console
Diagnostics RS-232
DCE,9600,n,8,1
Link
Act
Full
1 2 3 4 5 6 7 8
1x 2x 3x 4x 5x 6x 7x 8x
D-Link
Building Networks for People
DGS-3208
Configuration
Bridge
Broadcast Domains
Trunk
Monitor
User
Utilities
Help
Configuration
Bridge
Monitor
User
Web-Based Network Management
Introduction
The DGS-3208F offers an embedded Web-based (hypertext) interface allowing users to manage the Switch from anywhere on the network through a standard browser such as Netscape Navigator/Communicator or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the Switch using HTTP protocol. Your browser screen may vary with the screen shots (pictures) in this guide.
NOTE: This Web-based Network Management module does not accept Chinese language input (or other languages requiring 2 bytes per character).
Getting Started
The first step in getting started in using Web-based management for your Switch is to secure a browser. A Web browser is a program which allows a person to read hypertext, for example, Netscape Navigator or Microsoft Internet Explorer. Follow the installation instructions for the
Document: Done

A

TECHNICAL SPECIFICATIONS

General	
Standards:	IEEE 802.3z on each port IEEE 802.3 Frame types: Transparent IEEE 802.3 MAC layer frame size: 64–1518 bytes
Protocol:	CSMA/CD
Data Transfer Rate:	Gigabit Ethernet: 2000 Mbps (full duplex)
Topology:	Star
Network Cables:	525 m 50/125-mm, 275 m 62.5/125-mm multimode fiber
Number of Ports:	Eight (8) 1000-Mbps ports

Physical and Environmental	
AC inputs:	100 – 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	50 watts maximum
DC fans:	Three (3) built-in 40 x 40 mm fans
Operating Temperature:	0 ~ 50 degrees Celsius
Storage Temperature:	-25 ~ 55 degree Celsius
Humidity:	5% ~ 95% RH, non-condensing
Dimensions:	441 mm x 367 mm x 44 mm (1U), 19 inch rack-mount width
Weight:	4.8 kg
EMI:	FCC Class A, CE Mark Class A, VCCI Class A, BSMI Class A, C-Tick Class A
Safety:	UL (UL 1950), CSA (CSA950), TUV/GS (EN60950)

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	16 Mbytes per device *83.3 MHz
Filtering Address Table:	12K MAC address per device
Packet Filtering/Forwarding	1,416,202 pps per port

Performance	
Rate:	
MAC Address Learning:	Self-learning, auto-aging

INDEX

% of Utilization, 122
% Utilization, 80
%Util., 78

:Root Port, 22
:Spanning Tree Algorithm Protocol, 4
:Status, 59

1024-1518, 83, 128
128-255, 83
128–255, 127

256-511, 83, 128

512-1023, 83, 128

64, 83, 127
65-127, 83, 127

AC inputs, 137
AC Power Connector, 10
AC power cord, 5
Access Level, 132
Access Right, 76, 101
Access Rights
  read/write, 76
Accessory pack, 5
Action, 59, 60
Add/Modify User Account, 36, 37
Administrator, 15, 132
Administrator and Normal User Privileges, 34
Advanced, 96
Aging out of filtering information, 20
Aging Time
  very long, 20
  very short, 20
Aging Time, definition of, 20
Aging Time, range of, 20
Alleviating network loop problems, 24
Analysis, 127
Authentication Failure, 18
Automatic learning, 20
Automatic topology re-configuration
  Spanning Tree Algorithm, 21

Basic Setup, 94
Baud Rate, 43
Baud Rate, 103, 104
BOOTP (the BOOTstrap Protocol), 70
BOOTP broadcast, 41
BOOTP protocol, 41
BOOTP server, 41
BOOTP Service, 41
BPDU, 53, 108
Bridge, 106
Bridge Forward Delay, 23, 52
Bridge Forward Delay (4-30 Sec), 109

Bridge Hello Time, 23, 52
Bridge Hello Time (1-10 Sec), 109
Bridge Level, STA Operation Level
Root Bridge, 21
Bridge Max Age, 52
Bridge Max Age (6-40 Sec), 109
Bridge Max. Age, 23
Bridge MIB (RFC 1493), 4
Bridge Priority, 22
Bridge Priority, 23, 25
Bridge Priority (0-65535 Sec), 109
Bridge Priority(0-65535 Sec), 54
Bridge Priority(0-65535), 52
BridgeIdentifier, 22
Broadcast, 129
broadcast packets, 48, 49
Broadcast RX, 84
broadcast storm, 48
Broadcast Storm Falling Action, 47
Broadcast Storm Rising Action, 47
Broadcast TX, 84
Bytes Received, 124
Bytes Recv., 80
Bytes Sent, 80, 123

Changing the Protocol Parameters, 51, 55
Cold Start, 17
Collisions, 82, 126
Community, 100
Community name, definition of, 75
Community names
Private, 76
Public, 76
Community String, 76, 101
Config File Name, 72, 103
Configuration, 93
Configure Advanced Switch Features, 45
Configure Console, 42
Configure Filtering and Forwarding Table, 56, 58, 59
Configure IP Address, 40
Configure Port Mirroring, 49
Configure Ports, 46
Configure Spanning Tree Protocol, 50, 51, 55
Configure Switch, 44
Confirm New Password, 132
Connecting The Switch, 13
Connecting to the Switch VT100-compatible terminal, 30
Console, 103
Console Configuration, 42
Console LED indicator, 12
Console port (RS-232 DCE), 16
Console port settings, 16
Console Timeout, 43, 103, 104
Console Usage Conventions, 31
Cost, 56, 110
CRC + Alignment, 126
CRC Errors, 79, 80, 81, 83
Custom FDB, 113
Custom Filtering Table, 59, 60
Custom Forwarding Table, 58

Data Bits, 104
Data filtering rate, 4
Data forwarding rate, 4
data packet, 53, 108

Default Gateway, 42, 95
Designated Port, 22
Designated Root, 53, 108
DesignatedBridge, 22
Desktop or Shelf Installation, 6
Destination Address, 113
Destination IP Address, 73
Destination MAC Address, 58
Destination Port, 58, 113
Dimensions, 137
Download, 102
Dropped Frames, 82, 125
Dynamic filtering, 20
Dynamic Filtering, definition of, 59

Errors, 125
Ethernet interface
in-band communication, 40

Factory Reset to Default Value, 89
Falling Action, 49
FDB Table, 112
Features, 3
File Name, 72, 102
Filter Status, 114
Filter Table, 114
Filtering and Forwarding Table Configuration, 56, 58, 59
Filtering Database, 19
Firmware and Configuration Update, 70
Firmware Update, 71, 102
First time connecting to the Switch, 32
Flash memory, 4
Flow Control, 97, 104
Flow Ctrl, 47, 48
Forward Delay, 26
Forward Delay(4-30 sec), 52
Forward Delay(4-30 Sec), 54
Forward Delay(sec), 53, 108
Forwarding Table, 84, 97
Fragments, 81
Frames Received, 124
Frames Recv., 80
Frames Sent, 80, 124
Front Panel, 9
Full duplex, 4
Full/Half LED indicator, 12

General User, 132

Hardware Revision, 95
head of line (HOL) blocking prevention, 96
Head Of Line (HOL) Blocking Prevention, 46
heat dissipation, 6
Hello Time, 26
Hello Time(1-10 sec), 52
Hello Time(1-10 Sec), 54
Help, 134
Hold Time(Sec), 53, 108
Humidity, 137

Identifying External Components, 9
Illustration of STA, 24
Introduction, 1–4
IP address, 41
IP Address, 77, 95, 100
IP Addresses and SNMP Community Names, 16
IP Configuration, 40

Jabber, 125
Jabbers, 82

LAN card, 14
Last Detected Source Address, 125
Last Screen MAC, 123
Last Seen MAC, 80
Last TFTP Server Address, 103
Late Collision, 126
Late Collisions, 82
Learned, 85
LED Indicators, 11
Link Change Event, 18
Link Status, 123, 125
Link/Act LED indicator, 12
Local console management, 15
Lock Address Table(STOPs Learning), 57
Login On The Switch Console By Registered Users, 36
Login to DGS-3200 Manager, 92
Logout, 90
Lower Bridge Identifier, 22

MAC Address, 59, 60, 85, 114
MAC Address Age-out Time, 58
MAC Address Learning, 138
MAC Received Error, 126
Mac Rx Errors, 82
Management, 4
Management Information Base (MIB), 18
Max Age(6-40 sec), 52
Max Age(6-40 Sec), 54
Max Age(Sec), 53, 108
Max. Age Time, 26
MIB's Object-Identity (OID), 19
MIB-II (RFC 1213), 4
Monitor, 121
Multicast, 128
Multicast RX, 84
Multicast TX, 84

Network Classes
  Class A, B, C for Subnet Mask, 42
Network loop detection and prevention
  Spanning Tree Algorithm, 21
Network Monitoring, 77, 78, 80, 82, 84
New Password, 37, 132
New Root, 18
Normal User, 15

Old Password, 37, 132
Operating Temperature, 137
out-of-band management, 103
Out-of-Band Management, 15
Oversize Frames, 81, 126
Overview, 122
Overview of this User's Guide, v

Packet Forwarding, 19
Parity, 104
Path Cost, 110
Path Cost, 23
PC to Switch, 13
Performance features, 3
Performing a System Reset, 89
Ping Test, 72
Port, 59, 83, 85
Port (1-8), 47, 48
Port Error Packet Statistics, 80

Port Mirror, 99
Port Mirroring Configuration, 49
Port Packet Analysis Statistics, 82
Port Priority, 24, 26
Port Priority, 22
Port STP, 110
Port Traffic Statistics, 78, 79
Port type settings
  Console, 43
  Out-of-Band, 43
Port Utilization, 77
Ports, 79, 81
Ports Setup, 97
Power Consumption, 137
Power Failure, 8
Power LED indicator, 12
Power on, 8
Prevent Unauthorized Users, 32
Priority, 47, 48, 56, 98, 110
PROM Firmware Version, 94
Protocol Parameters
  Bridge Forward Delay field, 52
  Bridge Hello Time field, 52
  Bridge Max Age field, 52

Rack Installation, 7
RAM Buffer, 137
RE-232 DCE console port, 3
Read-only MIBs, Definition of, 19
Read-write MIBs, Definition of, 19
Rear Panel, 10
Received Bad Fragments, 126
Repetition, 73
Reset, 106
Resetting the Switch, 88
Rising Action, 48
RMON MIB (RFC 1757), 4
RMON probe, 50, 99
Root Bridge, 21
Root C, 53
Root Cost, 108
Root Path Cost, 22
root port, 108
Root Port, 53, 108
Root Priority, 54
Root Priority(Sec), 108
Routers, 3
RS-232 DCE console port, 15
Runtime Software Version, 94
RX (good), 128
RX (GOOD), 83
RX Bytes, 128
RX frames/sec, 122
RX Octets, 84
RX/sec, 78

Save, 105
Save Configuration, 35
Segments, Network, 2
Send Bootp Request Upon Power Up, 96
Serial Port, 43, 103, 104
Setting Up The Switch, 39
Setup, 6
Side Panels, 11
SLIP, 103
SLIP interface
  out-of-band communication, 40
SLIP management, 43, 104
sniffer, 50, 99
SNMP Community String, 76
SNMP Configuration, 75, 76
SNMP Manager, 101
Software Update Mode, 71, 102

Source Port, 50
Spanning Tree Algorithm (STA), 20
Spanning Tree Algorithm (STA), Function of the, 15
Spanning Tree Algorithm Parameters, 50
Protocol Parameters, 50
Spanning Tree Protocol, 52, 107, 110
Spanning Tree Protocol (STP), 53, 108
Speed, 79
Speed/Duplex, 47, 97
STA Operation Levels, 21
On the Bridge Level, 21
Standard MIB-II, 18
State, 47, 48
Static filtering, 20
Static Filtering, definition of, 59
Status, 77
Steps to Create Administrator or Normal User Access, 33
Stop Bits, 104
Storage Temperature, 137
Store and forward switching, 3
STP Custom Setting, 55
STP Parameters Setting, 51
STP State, 55, 110
subnet mask, 95
Subnet Mask, 42, 95
Switch Monitoring, 77
Switch STP, 107
Switch to Switch (other devices), 14
Switching Technology, 2
System Configuration, 39, 40, 42, 44, 46, 49, 51, 55, 56, 58, 59
System Contact, 44, 45, 94
System Description, 94
System Fans, 11
System Location, 44, 45, 94
System Name, 44
System Name, 44, 94
System OID, 94
System Restart Setting
Out-of-Band Baud Rate, 104
System Uptime, 94
System Utilities, 72

Target Port, 50
TCP/IP Setup, 95
TCP/IP TELNET protocol, 30
TECHNICAL SPECIFICATIONS, 136
TELNET program, 31
Terminal emulation/VT100, 16
Terminal emulator program
Under Windows operating system, 30
Terms used in document, v
TFTP (the Trivial File Transfer Protocol), 70
TFTP Server Address, 71, 102
Third-party vendors' SNMP software, 19
Threshold, Falling Action, 49
Threshold, Rising Action, 48
Time Since Topology Changes(sec), 53, 107
Topology Change, 18
Topology Change Count, 53, 108
Total Bytes Received, 124
Total Bytes Recv., 80
Total errors, 82
Total Errors, 126
Total Frames Received, 124

Total Frames Recv., 80
Total RX, 83, 84, 128
Traffic, 123
Traffic Statistics, 77, 79, 80, 82
Transmission Methods, 137
trap manager, 49
Trap Manager, 100
Traps, 17
Traps, definition of, 17
TX (good), 128
TX (GOOD), 83
TX Bytes, 128
TX frames/sec, 122
TX Octets, 84
TX/sec, 78

Unicast, 128
Unicast RX, 84
Unicast TX, 84
Unpacking, 5
Unpacking and Setup, 5–8
Update Interval, 78, 79, 81, 83, 127
Use Config File, 72, 103
User, 131
User Account Management, 36
User Name, 132
User-Changeblel Parameters, 23
Username, 37
Using the Console Interface, 30
Utilization, 123, 124

ventilation, 6
View/Delete User Account, 38
VT100-compatible terminal, 30

Warm Start, 18
Web browser, 91
Weight, 137

D-Link Offices

AUSTRALIA	**D-LINK AUSTRALASIA** Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand) WEB: www.dlink.com.au E-MAIL: info@dlink.com.au
CANADA	**D-LINK CANADA** 2180 Winston Park Drive, Oakville, Ontario L6H 5W1 Canada TEL: 1-905-829-5033 FAX: 1-905-829-5223 WEB: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca
CHILE	**D-LINK SOUTH AMERICA** Isidora Goyenechea #2934 of.702, Las Condes, Santiago, Chile TEL: 56-2-2323185 FAX: 56-2-2320923 WEB: www.dlink.cl
CHINA	**D-LINK CHINA** 15th Floor, Science & Technology Tower, No. 11, Baishiqiao Road, Haidian District, Beijing 100081 China TEL: 86-10-68467106-9 FAX: 86-10-68467110 WEB: www.dlink.co.cn
DENMARK	**D-LINK DENMARK** Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark TEL:45-43-969-040 FAX:45-43-424-347 WEB: www.dlink.dk
EGYPT	**D-LINK MIDDLE EAST** 7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt TEL: 202-2456176 FAX: 202-2456192 WEB: www.dlink-me.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 WEB: www.dlink-france.fr E-MAIL: info@dlink-france.fr
GERMANY	**D-LINK GERMANY** Bachstr. 22, D/65830 Kriftel Germany TEL: 49-(0)6192-97110 FAX: 49-(0)6192-971111 WEB: www.dlink.de BBS: 49-(0)6192-971199 (Analog) 49-(0)6192-9711 98 (ISDN) INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free)
INDIA	**D-LINK INDIA** Plot No.5, Kurla-Bandra Complex Road, Off Cst Road, Santacruz (E), Bombay - 400 098 India TEL: 91-22-6526578 FAX: 91-22-6528476 WEB: www.dlink.india.com
ITALY	**D-LINK ITALY** Via Nino Bonnet No. 6, 20154 Milano, Italy TEL: 39-2-2900-0676 FAX: 39-2-2900-1723 E-Mail: dlink@tin.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 WEB: www.d-link.co.jp
SINGAPORE	**D-LINK INTERNATIONAL** 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-774-6233 FAX: 65-774-6322 WEB: www.dlink.intl.com E-MAIL: info@dlink.com.sg
SWEDEN	**D-LINK SWEDEN** World Trade Centre P. O. Box 70396, 107 24 Stockholm Sweden TEL: 46-8-700-6211 FAX: 46-8-219-640 E-MAIL: info@dlink.se
TAIWAN	**D-LINK TAIWAN** 2F, No. 119 Pao-Chung Road, Hsin-Tien, Taipei, Taiwan TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 WEB: www.dlinktw.com.tw
U.K.	**D-LINK EUROPE** D-Link House, 6 Garland Road, Stanmore, London HA7 1DP U.K. TEL: 44-181-235-5555 FAX: 44-181-235-5500 WEB: 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 WEB: www.dlink.com E-MAIL: tech@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®