D-Link®

DES-6000
Modular Ethernet Switch
User's Guide

First Edition (June 2000)
6DES6000..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.

1. 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.

Trademarks

Copyright Statement

FCC Warning

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

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

CE Mark Warning

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

Warnung!

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

Precaución!

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

Attention!

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

Attenzione!

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

VCCI Warning

注意

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

BSMI Warning

警告使用者

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

TABLE OF CONTENTS

ABOUT THIS GUIDE

This User's Guide tells you how to install your Modular Ethernet Switch, how to connect it to your Ethernet network, and how to set its configuration using either the built-in console interface or Web-based management.

Conventions

References in this manual to the DES-6000 are frequently written simply as "Switch" or "Switches" where the text applies to both models. Model numbers are normally used only to differentiate between specific Switches where necessary.

Unless differentiated by model number, all information applies to both models.

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, side panels, optional plug-in modules, and LED indicators of the Switch.
- Chapter 4, "*Connecting the Switch*." Tells how you can connect the Switch to your Ethernet network as well as providing an informational cable length table.
- Chapter 5, "*Switch Management Concepts*." Talks about Local Console Management via the RS-232 DCE console port and other aspects about how to manage the Switch.
- Chapter 6, "*Using the Console Interface*." Tells how to use the built-in console interface to change, set, and monitor Switch performance and security.
- Chapter 7, "*Web-Based Network Management*." Tells how to manage the Switch through an Internet browser.
- Appendix A, "*Technical Specifications*." Lists the technical specifications of the Switch.
- Appendix B, "*RJ-45 Pin Specifications*." Shows the details and pin assignments for the RJ-45 receptacle/connector.
- Appendix C, "*Sample Configuration File*."
- Appendix D, "*Runtime Software Default Settings*."

1

INTRODUCTION

This section describes the features of the Switch, as well as giving some background information about Ethernet/Fast Ethernet, Gigabit Ethernet, and switching technology.

Fast Ethernet Technology

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-T, provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The dominating market position virtually guarantees cost effective and high performance Fast Ethernet solutions in the years to come.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

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 100Mbps Fast Ethernet and a one hundred-fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps 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 1000Mbps-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, Fast Ethernet, or Gigabit 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 (from one port to another) is automatically forwarded by the switch, without interfering with any other segments (ports). This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

For Fast Ethernet or Gigabit Ethernet networks, a switch is an effective way of eliminating problems of chaining hubs beyond the "two-repeater limit." A switch can be used to split parts of the network into different collision domains, for example, making it possible to expand your Fast Ethernet network beyond the 205 meter network diameter limit for 100BASE-TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks.

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 DES-6000 Modular switch is designed for easy installation and high performance in an environment where traffic on the network and the number of users increases continuously.

Switch features include:

Chassis

The chassis is the main unit that modules and power supplies are installed into. A CPU module and a power supply module come preinstalled in the chassis.

Chassis features include:

- Eight slots for installing networking modules (plus one slot reserved for the CPU)
- Two slots for installing redundant power supply modules
- 21.3 Gigabit/sec. (Gbps) backplane switching fabric
- Hot-swappable design for power supply modules
- Networking modules warm-swappable (except CPU module)
- Ears and screws for rack mounting

Modules

The following describes the optional plug-in modules available for the switch.

CPU Module

- A single CPU module must be present and must be installed in first (uppermost) slot.
- Layer 2 switching based on MAC address & VLAN ID.
- Store and Forward packet switching.
- Broadcast Storm rate filtering.
- Supports static filtering (based on MAC address).
- Supports IEEE 802.1Q VLAN (Static VLAN).
- Proprietary simplified Port-based VLANs
- IEEE 802.1d Spanning Tree support.
- Address table: 12K MAC address per switch
- 96 Static VLAN Entries (in IEEE 802.1Q VLANs mode)
- Supports 802.1p priority queuing (2 priority queues)
- Port Aggregation (Port-Trunking) Capability
- Port Mirroring
- IGMP snooping
- Head Of Line (HOL) Blocking Prevention
- RS-232 port for out-of-band management and system configuration
- Telnet Remote Configuration
- TFTP software upgrades, settings file and switch log uploads
- Web-based management
- SNMP Agents:
  - MIB-II (RFC 1213)
  - RMON MIB (RFC 1757)
  - Bridge MIB (RFC 1493)
- SLIP
- Supports four RMON (1,2,3,9) groups
- Port Security
- BootP support
- Support for DHCP Client

10BASE-T/100BASE-TX Module

- 16 10BASE-T/100BASE-TX ports
- Fully compliant with IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX
- All 10/100Mbps ports support NWay auto-negotiation
- Back pressure Flow Control support for Half-duplex mode
- IEEE 802.3x-compliant Flow Control support for Full-duplex
- Per port packet buffer: 0.5 Mbytes

100BASE-FX (MT-RJ) Module

- 12 100BASE-FX (MT-RJ) Fast Ethernet ports
- Fully compliant with IEEE 802.3u 100BASE-FX
- Back pressure Flow Control support for Half-duplex mode
- IEEE 802.3x compliant Flow Control support for Full-duplex
- Per port packet buffer: 0.5 Mbytes

1000BASE-SX (SC) Module

- 2 1000BASE-SX (SC) Gigabit Ethernet ports
- Fully compliant with IEEE 802.3z
- Support Full-duplex operation only
- IEEE 802.3x-compliant Flow Control support
- Per port packet buffer: 2 Mbytes

1000BASE-LX (SC) Module

- 2 1000BASE-LX (SC) Gigabit Ethernet ports
- Fully compliant with IEEE 802.3z
- Support Full-duplex operation only
- IEEE 802.3x-compliant Flow Control support
- Per port packet buffer: 2 Mbytes

Power Supply Modules

- Dual power modules design
- Current sharing design
- Full redundant feature design to ensure continuous operation
  - If one power module failed, the other will take over all current supply automatically.
- Hot-swappable/Hot-pluggable capability
- Power management functions enabled
- Revolving handle design
- Input: 90 ~ 264 VAC, 47 ~ 63Hz
- Output: 3.3V: 4A ~ 60A
- 12V: 0.1A ~ 2A

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 switch chassis
- One management module (pre-installed in uppermost slot)
- One power supply module (pre-installed)
- One mounting kit: four mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- One console cable
- One printed copy of the quickstart guide
- One printed copy of this user's guide
- One CD-ROM containing this user's guide

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

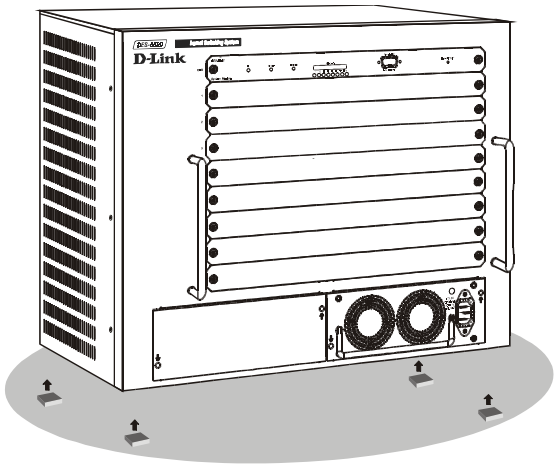


Figure 2-1. Switch installed on a Desktop or Shelf

Rack Installation

The Switch 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.

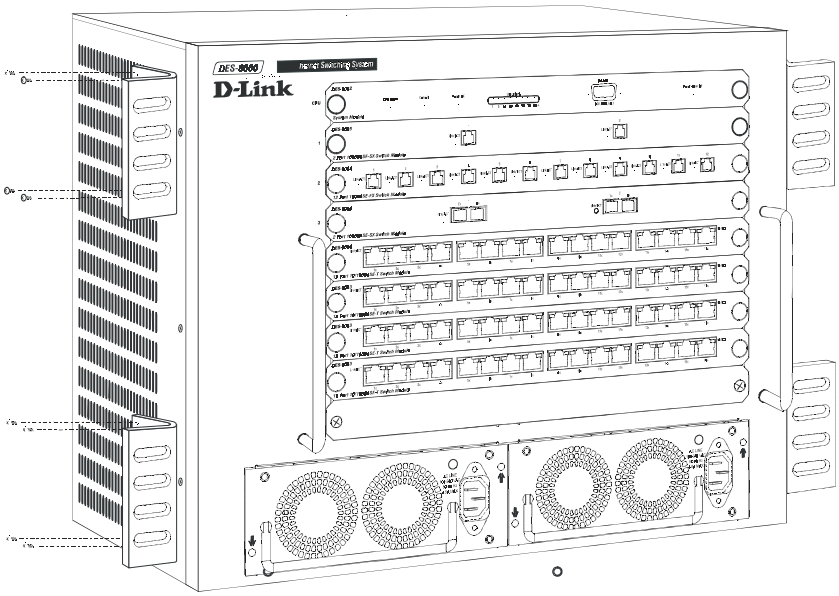


Figure 2-2. Attaching the mounting brackets to the Switch

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

Installing Modules

The DES-6000 supports up to 9 modules which can be installed into the module bays. Networking modules are warm-swappable, meaning they can be added and removed while power to the switch is ON. After warm-swapping a networking module, the switch will automatically be rebooted. Make sure to use the Save Changes command to save the current configuration to NV-RAM before warm-swapping modules. The CPU module, however, is NOT hot-swappable. Removing or inserting the CPU module while the power is on may cause irreparable damage to the module and/or to the Switch itself. Further, make sure you have unplugged the power cord from the removable power supply module before inserting or removing it from the Switch.

CAUTION: Due to the high energy present in this system, extreme caution should be exercised whenever adding or removing system components. No element of this system may be installed or removed except by an authorized technician.

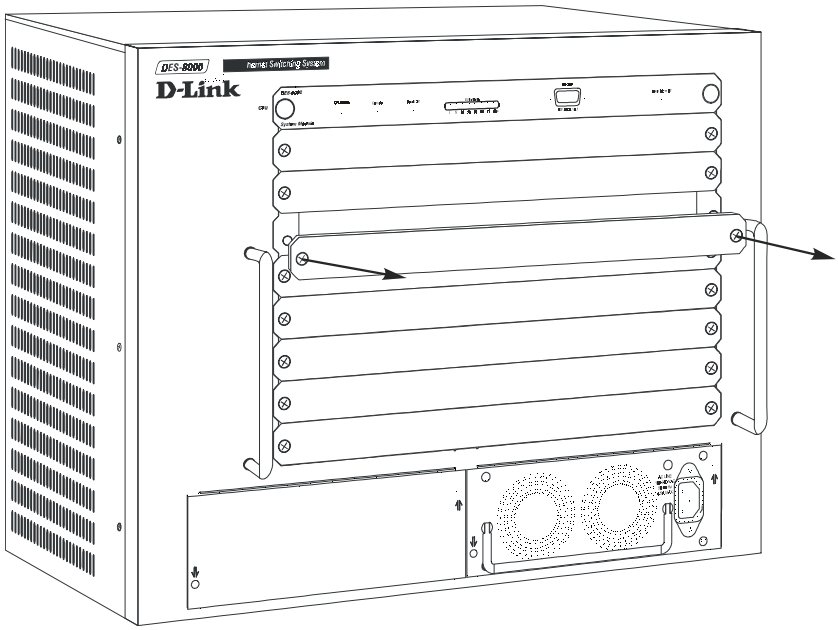


Figure 2-3. Removing a Blank Slot Cover

Modules can be installed into any free slot, except the CPU module which must be installed in the uppermost (top) slot. To install a module, simply remove a blank slot cover and slide the module along the guide rails until it snaps firmly in place.

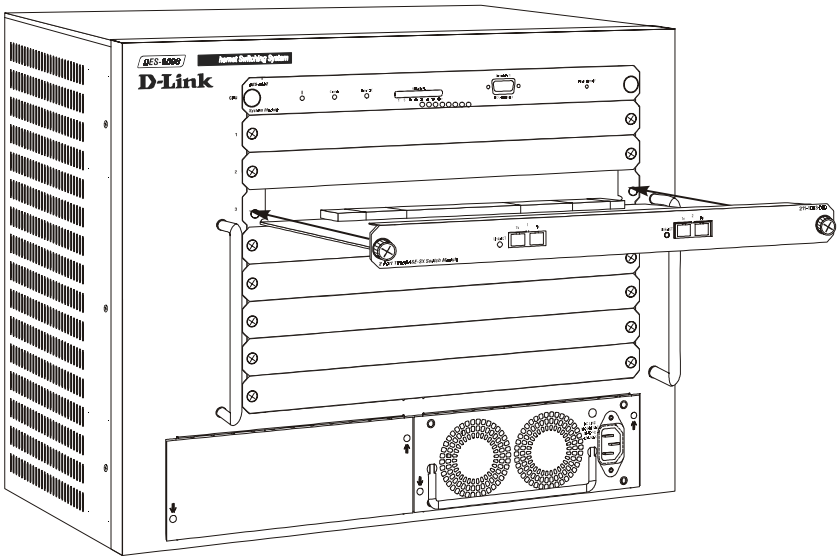


Figure 2–4. Installing a Module

Connecting a Terminal

The DES-6000 can perform basic switching functions without special configuration, but to use the Switch's advanced features you must first configure the unit through a terminal (a VT-100 serial data terminal or a computer running a VT-100 emulator). The connection is made through the Switch's Diagnostic RS-232 port, which is configured at the factory as follows:

- Baud Rate: 9600
- Data Bits: 8
- Parity: none
- Stop Bits: 1
- Flow Control: None

The RS-232 port has a nine-socket D-shell connector with IBM-type DCE wiring, and can be connected to the terminal using an off-the-shelf RS-232 cable with the proper connectors for the terminal and the DES-6000.

Power on

Power up the DES-6000 as follows:

1. Make sure the power module is properly installed in the device.
2. Plug the device end of the supplied power cord firmly into the power inlet on the DES-6000's front panel of the redundant power supply.
3. Plug the outlet end of the power cord firmly into a suitable AC outlet.
4. Observe the DES-6000's LED indicators to make sure the Switch is operating correctly.

The DES-6000's LED indicators operate as follows during a normal power-up:

- All indicators blink momentarily to indicate a system reset.
- The Power indicator flashes for about 20 seconds while the switch prepares its run-time software and performs a self-test.
- The Power indicator begins shining steadily, and the remaining indicators begin reflecting port and system status.

Power Failure

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

3

IDENTIFYING EXTERNAL COMPONENTS

This chapter describes the front panel, side panels, optional plug-in modules, and LED indicators of the Switch

Front Panel

The front panel of the Switch consists nine slide-in module slots for networking modules, two slide-in module slots for power supply modules, an RS-232 communication port, and LED indicators.

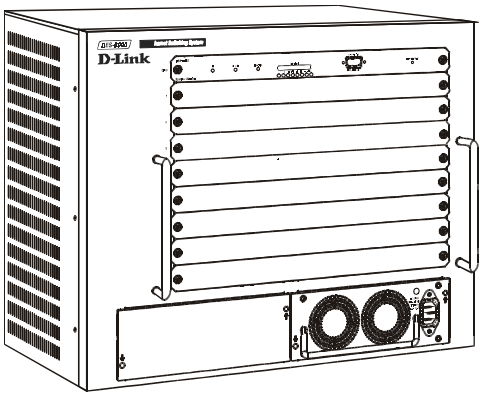


Figure 3-1. Front panel view of the Switch

- Comprehensive LED indicators display the conditions of the Switch and status of the network. A description of these LED indicators follows (see *LED Indicators*).
- An RS-232 DCE console port is used to diagnose the Switch via a connection to a terminal (or PC) and Local Console Management.
- Nine slide-in module slots installing networking modules and the CPU module.
- Two slide-in module slots for installing power supply modules.

Side Panels

The left side panel of the Switch contains four system fans. The right side panel contains heat vents.

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

Optional Plug-in Modules

The DES-6000 Modular Ethernet Switch is able to accommodate a range of plug-in modules in order to increase functionality and performance.

10BASE-T/100BASE-TX Module

Figure 3-2. 16-port, 10/100BASE-TX module

- 16-port, front-panel module.
- Connects to 10BASE-T and 100BASE-TX devices at full- or half-duplex.
- Supports Category 3, 4, 5 or better UTP or STP connections of up to 100 meters each.

100BASE-FX (MT-RJ) Module

Figure 3-3. 12-port, 100BASE-FX (MT-RJ) module

- 12-port, front-panel module.
- Connects to 100BASE-FX devices at full- or half-duplex.
- 12 100BASE-FX (MT-RJ) Fast Ethernet ports

- Fully compliant with IEEE 802.3u 100BASE-FX
- Back pressure Flow Control support for Half-duplex mode
- IEEE 802.3x compliant Flow Control support for Full duplex
- Per port packet buffer: 0.5 Mbytes
- Supports multi-mode fiber-optic cable connections of up to 412 meters in half-duplex or 2 km in full-duplex mode.

1000BASE-SX (MT-RJ) Gigabit Module

Figure 3-4. Two-port, 1000BASE-SX (MT-RJ) module

- Two-port, front panel module.
- Connects to a 1000BASE-SX device at full duplex.
- 2 1000BASE-SX (MT-RJ) Gigabit Ethernet ports
- Fully compliant with IEEE 802.3z
- Supports Full-duplex operation only
- IEEE 802.3x-compliant Flow Control support
- Per port packet buffer: 2 Mbytes

1000BASE-SX (SC) Gigabit Module

Figure 3-5. Two-port, 1000BASE-SX gigabit module

- Two-port, front-panel module.
- Connects to 1000BASE-SX devices at full duplex.
- 2 1000BASE-SX (SC) Gigabit Ethernet ports
- Fully compliant with IEEE 802.3z
- Support Full-duplex operation only
- IEEE 802.3x-compliant Flow Control support

- Per port packet buffer: 2 Mbytes

1000BASE-LX (SC) Gigabit Module

Figure 3-6. Two-port, 1000BASE-LX gigabit module

- Two-port, front-panel module.
- Connects to 1000BASE-LX devices at full duplex.
- 2 1000BASE-LX (SC) Gigabit Ethernet ports
- Fully compliant with IEEE 802.3z
- Supports full-duplex operation only
- IEEE 802.3x-compliant Flow Control support
- Per port packet buffer: 2 Mbytes

Power Supply Modules

- Dual power modules design with current sharing design
- Full redundant feature design to ensure continuous operation
  - If one power module failed, the other will take over all current supply automatically.
- Hot-swappable/Hot-pluggable capability
- Power management functions
- Input: 90 ~ 264 VAC, 47 ~ 63Hz
- Output: 3.3V: 4A ~ 60A
- 12V: 0.1A ~ 2A

LED Indicators

The LED indicators of the Switch include CPU Status, Console, Power OK, and Utilization. The following shows the LED indicators for the Switch along with an explanation of each indicator.

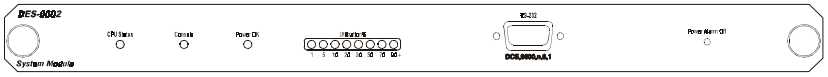


Figure 3-7. The Switch LED indicators

- **CPU Status** This leftmost indicator on the front panel displays the current status of the switch. The LED will blink while the Power-On Self-Test (POST) is running during startup. It will light a steady green after the POST test to indicate the switch is powered on and operating properly. It will light amber when an error occurs during startup and the switch is therefore not functioning.
- **Console** This indicator is lit green when the switch is being managed through the embedded console management program. The console program is accessed either through the out-of-band RS-232 console port using a straight-through serial cable or in-band via Telnet. When a secured connection is established, this LED is lit. The indicator blinks when the console RS-232 is accessed.
- **Power OK** This indicator lights green when the CPU module of the switch is receiving power and functioning properly.
- **Utilization** These indicators display the percentage of utilization on the CPU in the switch.

4

CONNECTING THE SWITCH

This chapter describes how to connect the Switch to your Ethernet network as well as providing an informational cable length table.

Switch to End Node

End nodes include PCs outfitted with a Network Interface Card (NIC) and most routers. For twisted-pair (copper) connections, the RJ-45 UTP ports on NICs and most routers are MDI-II. When using a normal straight-through cable, an MDI-II port must connect to an MDI-X port.

An end node can be connected to the Switch via a two-pair Category 3, 4, 5 UTP/STP straight cable (be sure to use Category 5 UTP or STP cabling for 100BASE-TX Fast Ethernet connections). The end node should be connected to any of the sixteen ports (1x - 16x) on the 10BASE-T/100BASE-TX module. The LED indicators for the port the end node is connected to are lit according to the capabilities of the NIC. 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 LED indicator states are possible for an end node to switch connection:

1. The 100M indicator comes *ON* for a 100 Mbps and stays *OFF* for 10 Mbps.

2. The Link/Act indicator lights up upon hooking up a PC that is powered on.

Switch to Hub or Switch

These connections can be accomplished in a number of ways. For twisted-pair (copper) connections, the most important consideration is that when using a normal, straight-through cable, the connection should be made between a normal crossed port (Port 1x, 2x, etc.) and an Uplink (MDI-II) port. If you are using a crossover cable, the connection can be made from a normal crossed port to another crossed port.

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

If the other switch or hub contains an unused Uplink port, we suggest connecting the other device's Uplink (MDI-II) port to any of the switch's (MDI-X) ports (1x - 16x 100BASE-TX ports).

If the other device does not have an unused Uplink port, make the connection with a crossover cable from any of the twisted-pair ports on the switch to any normal twisted-pair port on the hub.

10BASE-T Device

For a 10BASE-T device, the Switch's LED indicators should display the following:

- 100M speed indicator is *OFF*.
- Link/Act indicator is *ON*.

100BASE-TX Device

For a 100BASE-TX device, the Switch's LED indicators should display the following:

- 100M speed indicator is *ON*.
- Link/Act indicator is *ON*.

Cable Lengths

Standard	Media Type	MHz/km Rating	Maximum Distance
1000BASE-SX	50/125µm Multimode Fiber	400	500 Meters
	50/125µm Multimode Fiber	500	550 Meters
	62.5/125µm Multimode Fiber	160	220 Meters
	62.5/125µm Multimode Fiber	200	275 Meters
1000BASE-LX	50/125µm Multimode Fiber	400	500 Meters
	50/125µm Multimode Fiber	500	550 Meters
	62.5/125µm Multimode Fiber	500	550 Meters
	10µ Single-mode Fiber		5000 Meters
100BASE-FX	50/125µm Multimode Fiber (half-duplex operation)		400 Meters
	50/125µm Multimode Fiber (full-duplex operation)		2000 Meters
	62.5/125µm Multimode Fiber (half-duplex operation)		400 Meters
	52.5/125µm Multimode Fiber (full-duplex operation)		2000 Meters
100BASE-TX	Category 5 UTP Cable (100Mbps)		100 Meters
10BASE-T	Category 3 UTP Cable (10Mbps)		100 Meters

5

SWITCH MANAGEMENT CONCEPTS

This chapter discusses many of the features used to manage the switch, and explains many concepts and important points regarding these features. Configuring the Switch to implement these concepts is discussed in detail in the next chapters.

Local Console Management

Local console management involves the administration of the Switch via a direct connection to the RS-232 DCE console port. This is an Out-Of-Band connection, meaning that it is on a different circuit than normal network communications, and thus works even when the network is down.

The local console management connection involves a terminal or PC running terminal emulation software to operate the Switch's built-in console program (see Chapter 6, "*Using the Console Interface*"). Using the console program, a network administrator can manage, control and monitor the many functions of the Switch.

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

Diagnostic (Console) Port (RS-232 DCE)

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

The console port is set for the following configuration:

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

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

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

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, etc.). You must provide the switch with an IP Address to meet the specification of your networking address scheme.

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

For security, you can set in the Switch a list of IP Addresses of the network managers that 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

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.

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

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 Power-On Self-Test (POST) is skipped.
- ♦ **Authentication Failure** This trap signifies that someone has tried to logon to the switch using an invalid SNMP community name. The switch automatically stores the source IP address of the unauthorized user.
- ♦ **New Root** This trap indicates that the Switch has become the new root of the Spanning Tree, the trap is sent by 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.
- **Port Partition** This trap is sent whenever a port is partitioned as a result of more than sixty-two collisions on the port (i.e., is automatically partitioned). The number of collisions that triggers this trap is the same at either 10Mbps or 100Mbps.
- **Broadcast Storm** This trap is sent whenever the port reaches the broadcast storm rising or falling threshold.
- **Power Supply Module Inserted** This trap is sent whenever a redundant power supply module is installed in the switch.
- **Power Supply Module Removed** This trap is sent whenever a redundant power supply module is removed in the switch.
- **Bad Power** This trap is sent whenever a redundant power supply is receiving AC power but not supplying DC power to the switch.
- **Power Supply Module Inserted** This trap is sent whenever a redundant power supply is installed in the switch.
- **Power Supply Module Temperature Warning** This trap is sent whenever the temperature of a redundant power supply module measures over 80° C (176° F).
- **Power Supply Module Voltage Warning** This trap is sent whenever a redundant power supply generates DC current over 3.9 volts.
- **Power Supply Module Current Warning** This trap is sent whenever a redundant power supply generates DC current over 60 amps.
- **System Fan Failure** This trap is sent whenever one of the four system fans in the switch fails.
- **Power Fan1 Failure** This trap is sent whenever one of the two fans on a redundant power supply module fails.
- **Power Fan2 Failure** This trap is sent whenever one of the two fans on a redundant power supply module fails.

MIBs

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

Read-only MIBs variables can be either constants that are programmed into the Switch, or variables that change while the Switch is in operation. Examples of read-only constants are the number of 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 learns the network configuration and uses this information 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 a station on Port 2, the Switch transmits that packet through Port 2 only, and transmits nothing through the other ports.

Aging Time

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

The Aging Time can be from 10 seconds to 9999 seconds. A very long Aging Time can result with the out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions.

On the other hand, 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, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Filtering Database

A switch uses a filtering database to segment the network and control communications between segments. It also filters packets off the network for intrusion control (MAC Address filtering).

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

For intrusion control, whenever a switch encounters a packet originating from or destined to a MAC address defined by the user, the switch will discard the packet.

Filtering includes:

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

Spanning Tree 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. The 1000Mbps segment has an assigned Path Cost of 4, the 100Mbps segment has an assigned Path Cost of 19, and each 10Mbps segment has an assigned Path Cost of 100, based on the STA specifications.

User-Changeable STA 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*:** 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*.

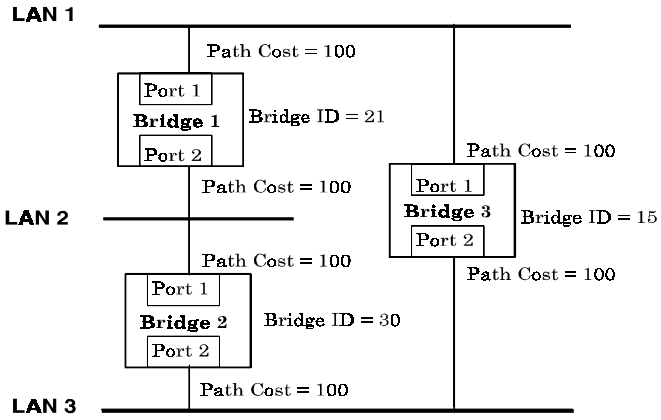


Figure 5-1. Before Applying the STA Rules

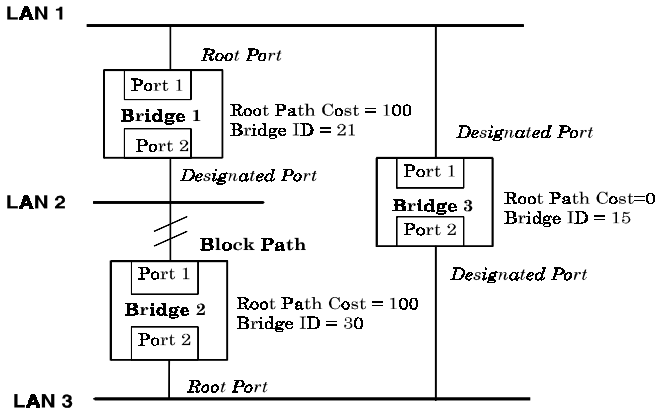


Figure 5-2. After Applying the STA Rules

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, with one port designated as the *anchor* of the group. Since all members of the trunk group must be configured to operate in the same manner, all settings changes made to the anchor port are applied to all members of the trunk group. Thus, when configuring the ports in a trunk group, you only need to configure the anchor port.

The Switch supports up to 16 trunk groups. Each module on the switch supports up to two trunk groups except gigabit modules, which don't support trunk groups. The Switch treats all ports in a trunk group as a single port. As such, trunk ports will not be blocked by Spanning Tree.

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

VLANs & Broadcast Domains

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

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

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

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

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

MAC-based Broadcast Domains

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

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

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

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

802.1Q VLANs

The Switch supports up to 2048 802.1Q VLANs. 802.1Q VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

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

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

802.1Q VLAN Segmentation

The following example is helpful in explaining how 802.1Q VLAN segmentation works. Take a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2 and has the Port VLAN ID number 2 (PVID=2). If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2, because it's Port VLAN ID number is 2 (PVID=2).

Sharing Resources Across 802.1Q VLANs

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

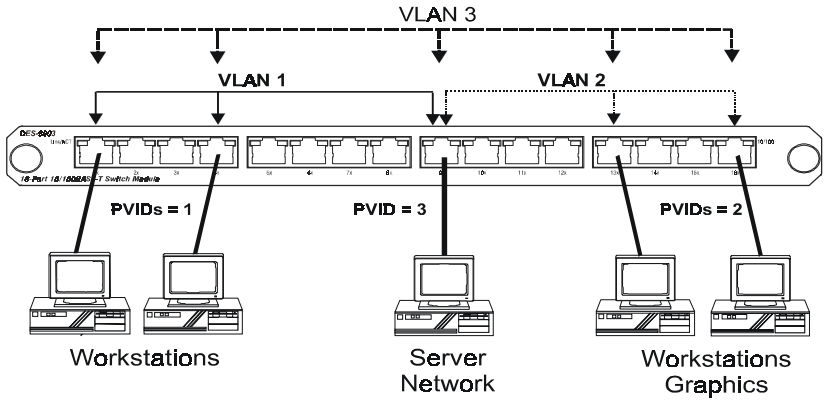


Figure 5-3. Example of typical VLAN configuration

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

Port	*PVID*
Port 1	1
Port 4	1
Port 13	2
Port 16	2
Port 9	3

Ports	*VID*
1,4,9	1
9,13,16	2
1,4,9,13,16	3

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

The server attached to Port 9 is shared by VLAN 1 and VLAN 2 because Port 9 is a member of both VLANs (it is listed as a member of VID 1 and 2). Since it can receive packets from both VLANs, all ports can successfully send packets to it. Ports 1 and 4 send these packets on VLAN 1 (their PVID=1), and Ports 13 and 16 send these packets on VLAN 2 (PVID=2). The third VLAN (PVID=3) is used by the server to transmit files that had been requested on VLAN 1 or 2 back to the computers. All computers that use the server will receive transmissions from it since they are all located on ports which are members of VLAN 3 (VID=3).

802.1Q VLANs Spanning Multiple Switches

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

Definitions of relevant terms are as follows:

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

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

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

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

VLANs Over 802.1Q-compliant Switches

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

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

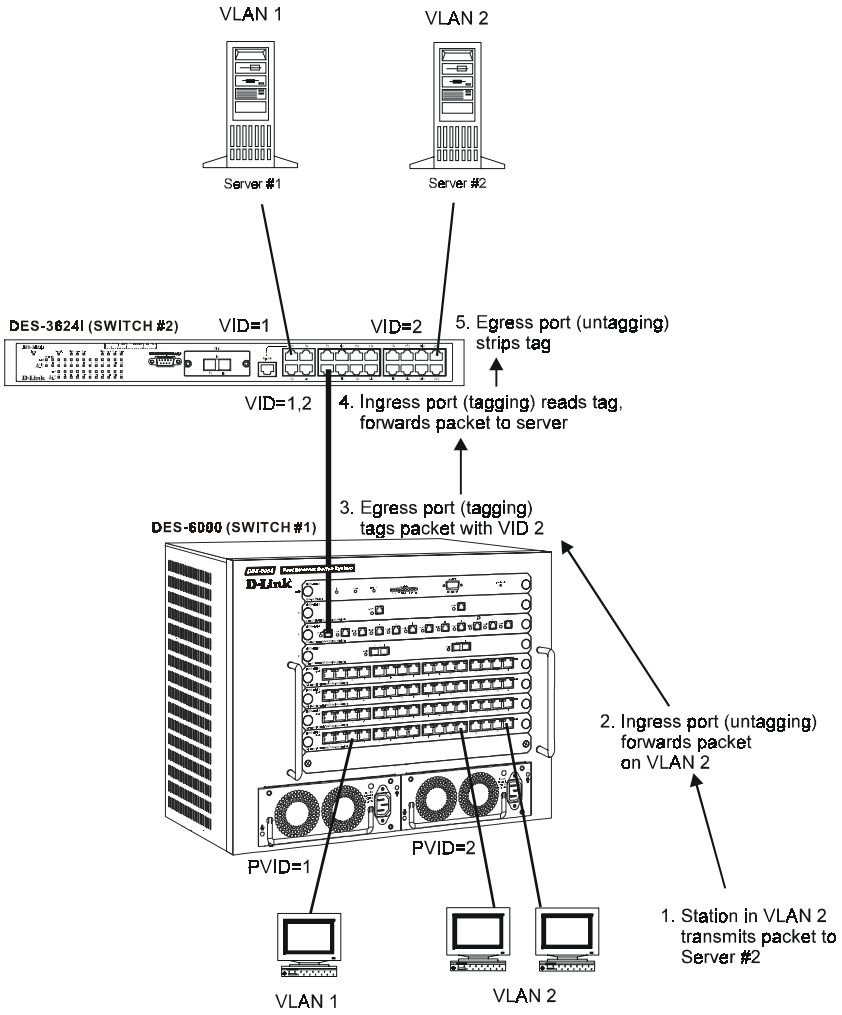


Figure 5-4. Data transmissions between 802.1Q-compliant switches

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

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

Port-based VLANs

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

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

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

To setup port-based VLANs, simply select one of 24 VLAN ID numbers, name the VLAN and specify which ports will be members. All other ports will automatically be forbidden membership, even dynamically as a port can belong to only one VLAN.

Broadcast Storms

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

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

Broadcast storms have long been a concern for network administrators with routers traditionally being used to prevent their occurrence, and if that failed, to at least limit their scope. However, with the advent of VLANs, switches are now able to limit broadcast domains better and cheaper than routers. Also, many switches, including the DES-6000 series, have broadcast sensors and filters built into each port to further control broadcast storms.

Segmenting Broadcast Domains

VLANs can be used to segment broadcast domains. They do this by forwarding packets only to ports in the same VLAN. Thus, broadcast packets will only be forwarded to ports that are members of the same VLAN. Other parts of the network are effectively shielded. As a result, the smaller the broadcast domain, the less effect a broadcast storm will have. Because VLANs are implemented at each switch port, they can be quite effective in limiting the scope of broadcast storms.

Eliminating Broadcast Storms

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

In the DES-6000 switch, the default rising threshold is met when more than 500 broadcast packets per second are being detected on a specified port. Once the rising threshold is surpassed for a duration of more than 5 seconds, it will trigger the broadcast storm rising action configured by the user. The default falling threshold is met if there are less than 250 broadcast packets per second. It is triggered once the duration is at least 30 seconds. The actions can easily be defined by using a normal SNMP management program or through the console interface.

6

USING THE CONSOLE INTERFACE

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

Setting Up A Console

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

1. Obtain suitable cabling for the connection.

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

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

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

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

A typical console connection is illustrated below:

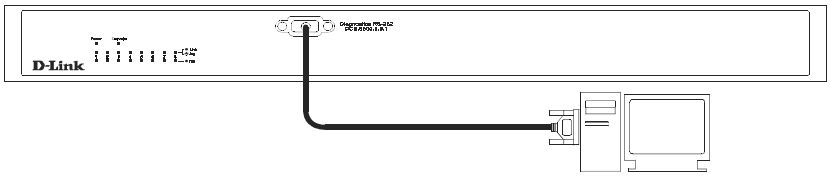


Figure 6-1. Example of a console connection

Connecting to the Switch Using Telnet

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

Console Usage Conventions

The console interface makes use of the following conventions:

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

Please note that the command APPLY only applies for the current session. Use **Save Changes** from the main menu for permanent changes. An asterisk "*" indicates a change has been made but won't take effect until the Switch has been rebooted.

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). Press Ctrl+R (hold down the Ctrl key, press the R key, and release both keys) to call up the screen, if the initial login screen does not appear. Also Ctrl+R can be used at any time to refresh the screen.

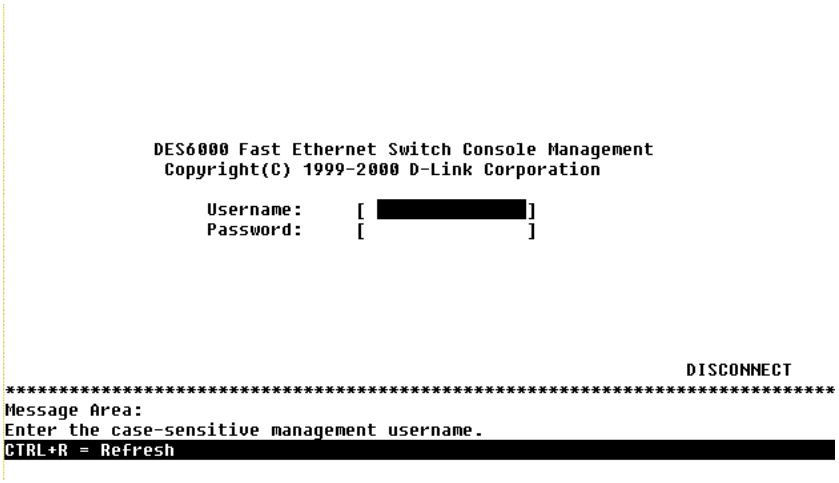


Figure 6-2. Initial Screen, first time connecting to the Switch

Press <Enter > or <Return> in the username and password fields. You will be given access to the main menu shown below:

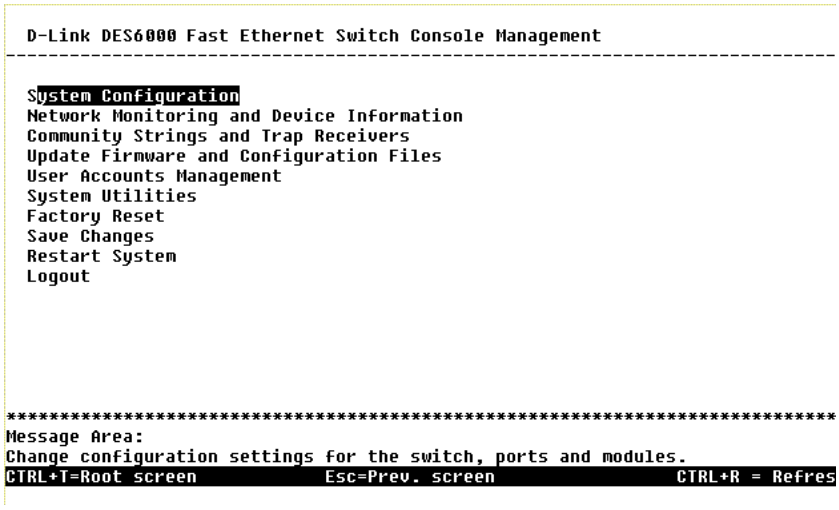


Figure 6-3. Main Menu

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

User Accounts Management

User accounts are accounts setup on the Switch which allow access to the switch management features.

From the screen above, move the cursor to the **User Accounts Management** menu and press Enter, then the **Users Accounts Management** menu appears.

1. Choose **Create/Modify User Accounts** from the **User Accounts Management** menu and the **Add/Modify User Accounts** 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 Accounts**. The **View/Delete User Accounts** 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	Read/Write	Yes, read only.
Network Monitoring	Read/Write	Yes, read only.
Community Strings and Trap Stations	Read/Write	Yes, read only.
Update Firmware and Configuration Files	Read/Write	Yes, read only.
User Accounts Management		
Create/Modify User Accounts	Read/Write	No
View/ Delete User Accounts	Read/Write	No
System Utilities	Read/Write	Yes, (Ping Test); read only for rest.
Factory Reset	Read/Write	No
Restart System	Read/Write	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 (see below). Pressing any key will return to the main menu. You are now ready to operate the Switch.

Save Changes

The Switch has two levels of memory normal RAM and non-volatile or NV-RAM. Settings need to be changed in all screens by clicking on the *Apply* button. When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect. Some settings, though, require you to restart the Switch before they will take effect. Restarting the Switch will erase all settings in RAM and reload them from the NV-RAM. Thus, it is necessary to save all settings to the NV-RAM before restarting the Switch.

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

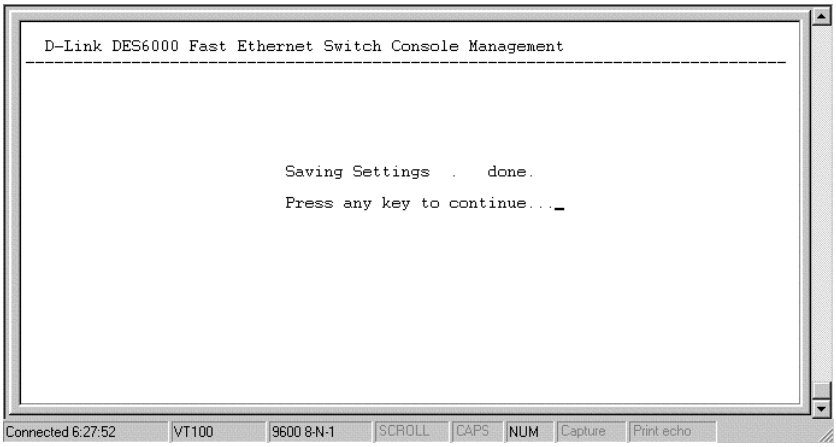


Figure 6-4. Save Changes screen

After the settings have been saved to NV-RAM, they will become the default settings for the Switch, and they will be used every time it is powered on, reset or rebooted. The only exception to this is a factory reset, which will clear all settings and restore them to their initial values listed in the Appendix, which were present when the Switch was purchased.

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.

Create/Modify User Accounts

To add or change your user password:

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

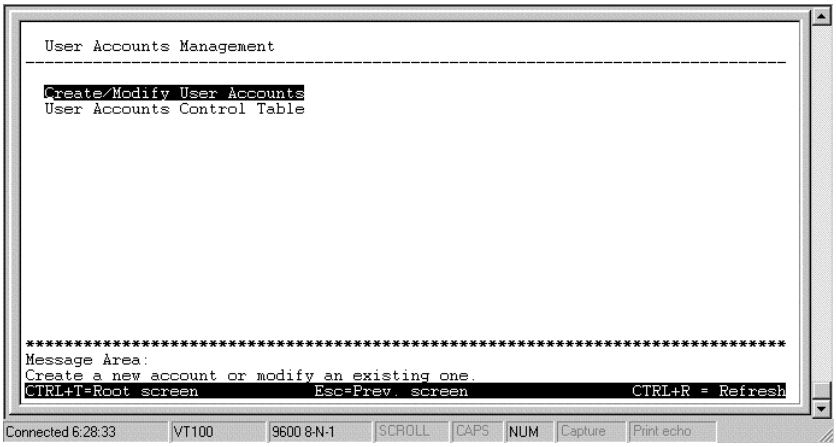


Figure 6-5. User Accounts Management menu

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

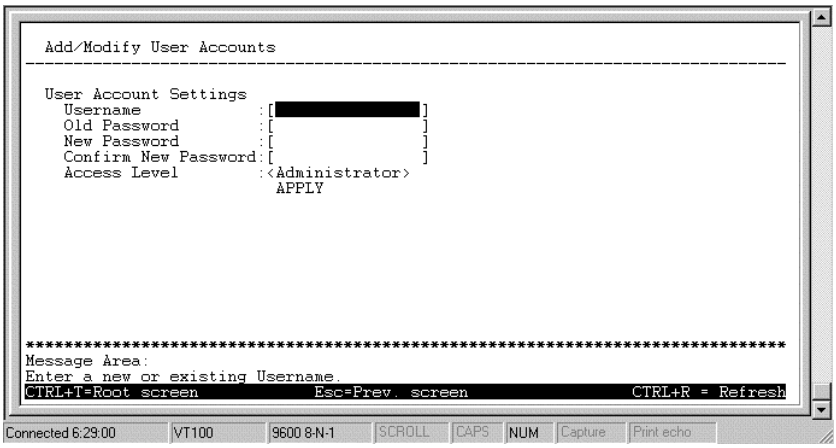


Figure 6-6. Add/Modify User Accounts screen

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

4. If you are an old 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.

User Accounts Control Table

Access to the console, whether using the console port or via Telnet, is controlled using a user name and password. Up to three of these 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 a user account:

Choose **User Accounts Control Table** from the **User Accounts Management** menu. The following screen appears:

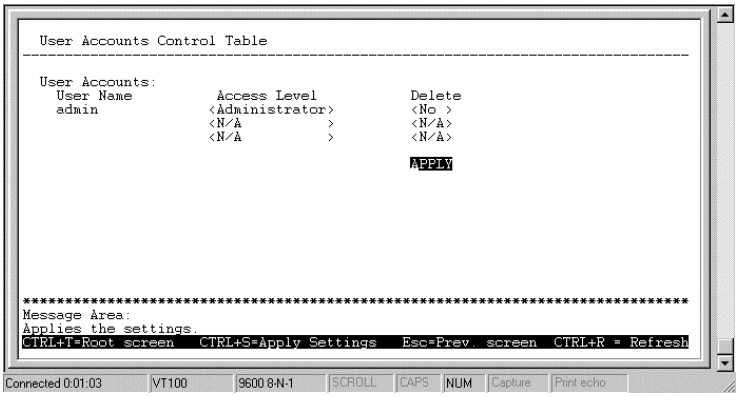


Figure 6-7. User Accounts Control Table

This screen is used to configure a users access level and delete user accounts.

To change a users access level, place the cursor on the access level field for the user and press the <space bar> to toggle.

To delete a user account, toggle the Delete field of the user you wish to remove to *Yes*.

Press APPLY to let the changes take effect.

Setting Up The Switch

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

System Configuration

Choose **System Configuration** to access the first item of the Switch's main menu. The following menu appears:

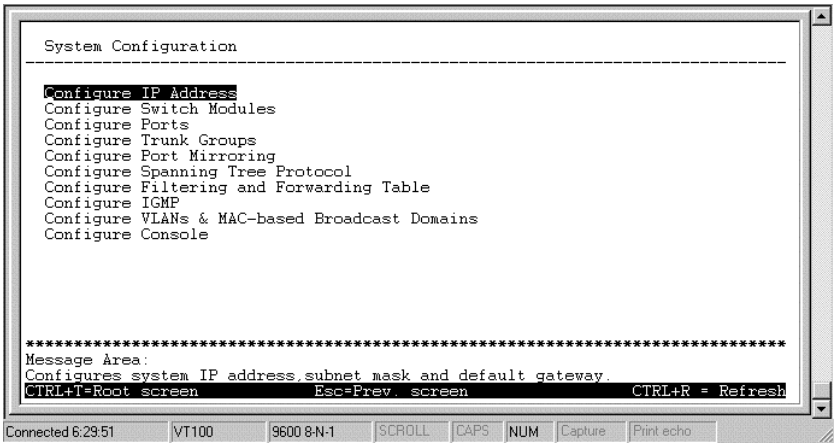


Figure 6-8. System Configuration menu

You will need to change some settings to allow you to be able to manage the Switch from an SNMP-based Network Management System or to be able to access the Switch using the Telnet protocol. See the next chapter for Web-based network management information.

Configure IP Address

The Switch needs to have a TCP/IP address assigned to it so that an in-band network management system (Web-based, Telnet, etc.) can find it on the network. The **IP Address 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:

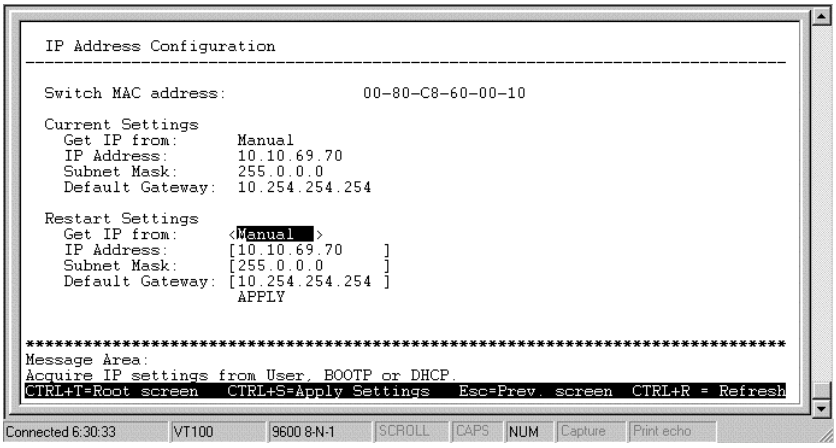


Figure 6-9. IP Address Configuration screen

The fields listed under the Current Settings heading are those that are presently being used by the Switch. Those fields listed under the Restart Settings heading will be used after the Switch has been restarted. Fields that can be set include:

- **Get IP from** Determines whether the Switch should get it's IP Address settings from the user (*Manual*), a *BootP* server, or a *DHCP* server.

  Manual – When manual is chosen, the switch will use the IP Address, Subnet Mask and Default Gateway settings defined in this screen upon being rebooted.

BootP – Sends 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.

DHCP – Causes the switch to act as a DHCP client and obtain IP settings from the DHCP server on your network.

- **IP Address** Determines the IP address used by the Switch for receiving SNMP and Telnet communications. These fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number between 0 and 255. This address should be a unique address on the network. The same IP address is shared by both the SLIP and Ethernet network interfaces.
- **Subnet Mask** Bitmask that determines the subnet that the Switch is on. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number between 0 and 255. If no subnetting is being done, the value should be 255.0.0.0 for a Class A network address, 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 you can leave this field blank.

Configure Console

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

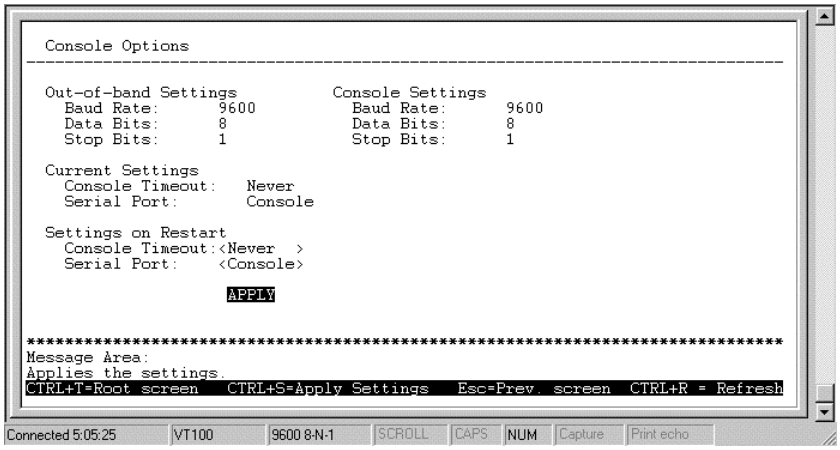


Figure 6-10. Console Options screen

The following fields can be set:

Settings on Restart:

- **Console Timeout** This is a security feature which measures the time that the console connection is inactive. Possible values are *2 mins*, *5 mins*, *10 mins*, *15 mins*, or *Never*. After the time expires the console will automatically log off.
- **Serial Port** Determines whether the RS-232 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 C*onsole.*
- **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 in SLIP mode; it does not apply when the port is set for

Console. Available speeds are 2400, 9600, 19,200 and 38,400 bits per second. The default setting in this Switch version is 9600.

The top of the screen displays the current settings for **Console Timeout** and **Serial Port** as well as the **Baud Rate**, **Data Bits**, and **Stop Bit** for Out of Band and Console settings, respectively.

Configure Switch Modules

The **Switch Module 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 these settings to be used for network management purposes.

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

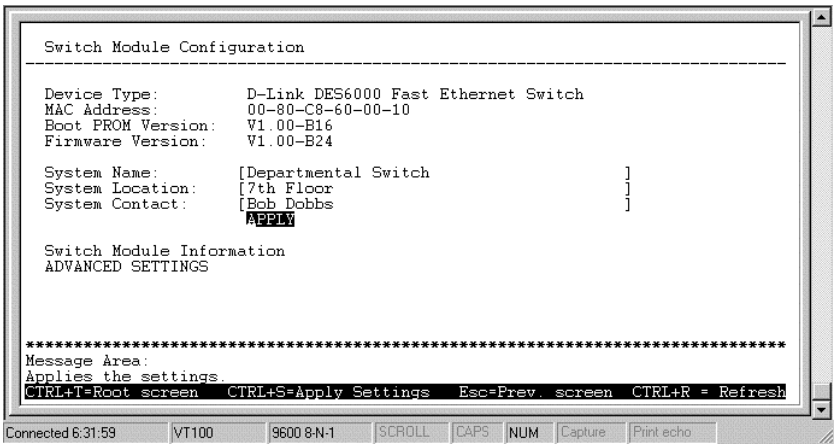


Figure 6-11. Switch Module Configuration screen

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.

Switch Module Information

This screen allows you to view information for each module in your switch, including the **Module**, **Type**, and **Hardware Version**. Press Switch Module Information on the **Switch Module Configuration** screen to access the **Switch Module Information** screen:

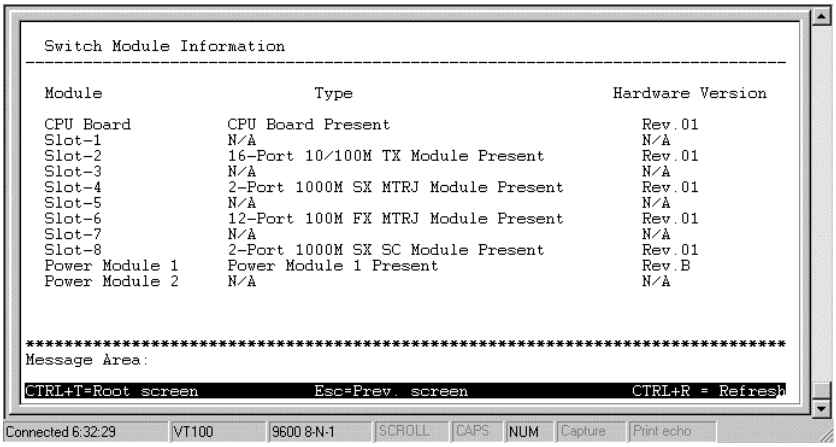


Figure 6-12. Switch Module Information screen

Advanced Settings

The **Configure Advanced Switch Features** screen allows you to set Head Of Line Blocking Prevention as well as to enable or disable auto-partitioning on all ports. Press ADVANCED SETTINGS on the **Switch Module Configuration** screen to access the **Configure Advanced Switch Features** screen:

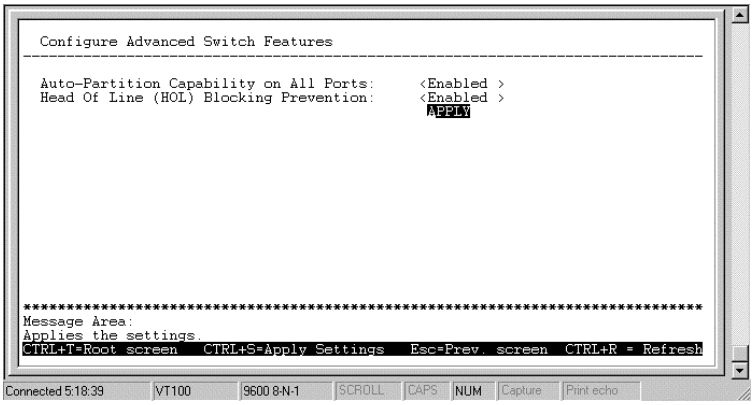


Figure 6-13. Configure Advanced Switch Features screen

The fields you can set are:

- **Auto-Partition Capability on All Ports** When this function is enabled, if too many consecutive collisions occur on an individual port, the port will be blocked off until a good packet is seen on the wire. If a port is partitioned, the Switch can only transmit data onto the connected segment, not receive it.
- **Head Of Line (HOL) Blocking Prevention** Enables or disables Head-Of-Line Blocking Prevention. Head-of Line blocking occurs when a packet originating on Port 1, for instance, needs to be forwarded to Ports 2 and 3. If Port 2 is occupied (causing the packet to be held in memory until the port is free), the packet destined for Port 3 will also be delayed, even though Port 3 may be free. Cumulatively, these delays can have a noticeable effect on overall network performance. Enabling HOL Blocking Prevention prevents Head-of-Line blocking from occurring, meaning that the packet destined for Port 3 gets delivered immediately.

Configure Ports

The **Port Configuration** screen allows you to change settings for a particular port.

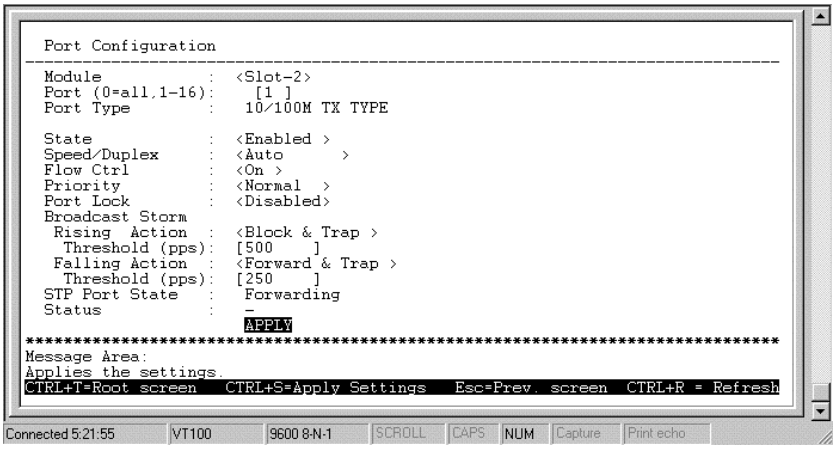


Figure 6-14. Port Configuration screen

Items in the above window are defined as follows:

- **Module** Specify the module containing the port you wish to configure.
- **Port** Specify the port you wish to configure.
- **Port Type** Specifies the speed and cable type of the selected port.
- **State** Enables or disables the port. This amounts to turning the port on or off.
- **Speed/Duplex** Selects the desired Speed and Duplex settings for the port. Possibilities include: *Auto*, *100M/Full*, *100M/Half*, *10M/Full*, or *10M/Half*. Choosing *Auto* enables NWay auto-configuration on the port. If the port is a Gigabit Ethernet port, *1000M/Full* will be displayed in this field.
- **Flow Ctrl** Toggles flow control *On* or *Off*. Flow control is useful during periods of heavy network activity when the Switch's buffers can receive too much traffic and fill up faster than the Switch can forward the information. In such cases, the Switch will intervene and tell the transmitting device to pause to allow the information in the port buffer to be sent.
- **Priority** Selects *Normal*, *High* or *Low*. The Switch has two packet queues where incoming packets wait to be processed for forwarding; a high priority and low priority queue. The high priority queue should only be used for data in which latency can have adverse affects on the function of an application, such as video or audio data, where latency can produce distorted sounds and images. Packets in the low priority queue will not be processed unless the High priority queue is empty. Setting the port priority to *High* will deliver all packets arriving at the port to the high priority queue, a *Low* setting will send them all to the low priority queue. The *Normal* setting causes the port to examine the packet for an IEEE 802.1p/Q priority tag. If no tag exists, the packet will be sent to the low priority queue. If the priority tag field in the packet header contains a value of 0-3, the packet will be placed in the low priority queue; a value of 4-7 causes the packet to be placed in the high priority queue.
- **Port Lock** When *Enabled*, automatic learning for all stations connected to this port will stop and entries in the Forwarding Table for all devices residing on this port will age out. The only traffic this port will allow is traffic from machines whose MAC address is manually entered in the Static Forwarding Table.
- **Broadcast Storm Rising Action** This setting will be activated when a Broadcast Storm Rising Threshold is met. When triggered, the port can be configured to *Do Nothing*, *Blocking* or *Block & Trap*. The *Do Nothing* setting causes the switch to operate normally, in other words, ignore the broadcast storm condition. The *Blocking* setting causes the port to drop all broadcast frames, thus isolating the broadcast storm. *Block & Trap* performs the same action as *Blocking*, except it also sends a trap to the designated Trap Recipient informing them of the situation. For more information on broadcast storms, please refer to the previous chapter.

- **Broadcast Storm Rising Threshold** This setting defines a ceiling for the number of broadcast packets per second on this port. Once met, the *Broadcast Storm Rising Action* (above) will be triggered. The assigned number should be high enough to allow normal broadcast packets (which comprise significant traffic) to be let through, while being low enough so that broadcast storms can be detected early.

- **Broadcast Storm Falling Action** This setting will be activated when the Broadcast Storm Rising Threshold and then the Broadcast Storm Falling Threshold are *each* met. This setting can be configured to *Do Nothing*, *Forwarding* or *Forward & Trap*. The *Do Nothing* setting causes the switch to operate normally, that is, to ignore the situation. If the port had met the *Broadcast Storm Rising Action* criteria and started *Blocking* broadcast packets, it will continue doing so. The *Forwarding* setting causes the port to begin forwarding broadcast frames, thus removing the *Blocking* state imposed by the *Broadcast Storm Rising Action*. *Forward & Trap* performs the same action as *Forwarding*, except it also sends a trap to the designated Trap Recipient informing them of the situation.

- **Broadcast Storm Falling Threshold** This setting defines the number of broadcast packets per second on this port which will trigger the *Broadcast Storm Falling Action* (above). This threshold will only trigger an action if the *Broadcast Storm Rising Threshold* has first been reached. The assigned number should be high enough to allow normal broadcast packets (which comprise significant traffic) to be let through as early as possible, while being low enough so that broadcast storms are completely eliminated.

- **STP Port State** This setting displays the ports current state as controlled by the Spanning Tree Protocol.

- **Link Status** The current speed, duplex mode and flow control status for the specific port. Press APPLY to refresh the link status after changing settings.

Press APPLY to let the changes take effect. If you wish these changes to become permanent, return to the main menu and choose **Save Changes**.

Configure Trunk Groups

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 "*Switch Management Concepts*" chapter of this manual.

The switch supports 2 trunk groups per module.

To set up a trunk group, choose **Configure Trunk Groups** on the **System Configuration** menu. The following screen appears:

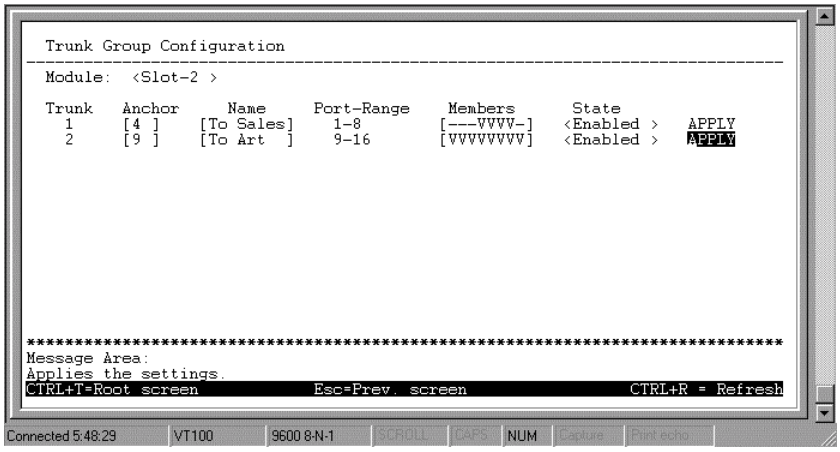


Figure 6-15. Trunk Group Configuration screen

The fields you can set are:

- **Anchor** The anchor port is the master port of the trunk group. Since all ports in a trunk group must have the same settings, any changes made to the settings of the anchor port will automatically be applied to all ports in the group. The anchor port must fall within the port range and be included as a member port.
- **Name** Enter the desired group name. In the example pictured above the first trunk group designates a trunk connection to a switch in the Sales department.
- **Members** Select between 2 to 8 ports to be members of the trunk group. In the example above, the first trunk group can comprise ports 1-8, as shown in the Port Range field. The 8 dashes (-) in the members field represent the 8 ports that can be members of the group; the first dash represents Port 1, etc. Position the cursor over the dashes representing ports you wish to be members and hit the <space bar>. This changes the dash to a 'V' and designates the port as a member of the trunk group.
- **State** Enables or disables this trunk group. Be careful when disabling trunk groups as the connections will return to normal operation and may cause signal loops. *Clear* will deselect all ports and erase the name of the trunk group.
- **Port Range** is a read-only field which lists the ports that can be members of the trunk group.

  Press APPLY to let the changes take effect.

Configure Port Mirroring

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

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

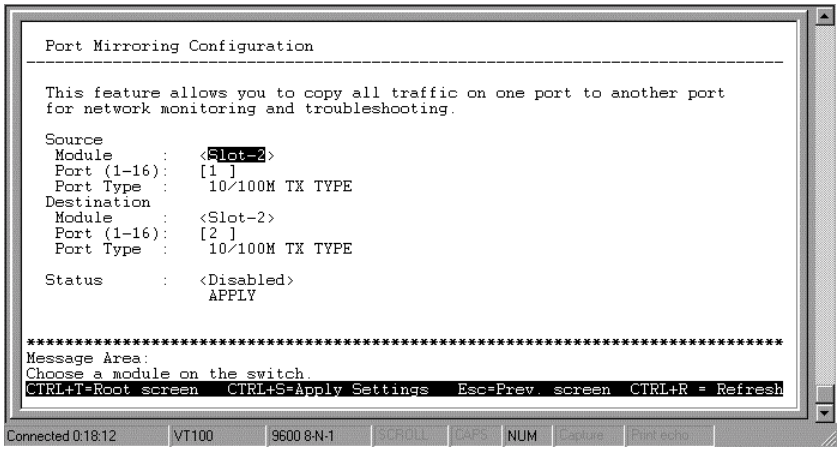


Figure 6-16. Port Mirroring Configuration screen

To configure a mirror port, select the Module, and Port from where you want to copy frames in the Source fields. Then select the Module and Port which receive the copies from the source port in the Destination fields. The destination (or target) port is where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe.

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

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 the previous chapter. It is recommended that you read this, as well as the introductory section in the same chapter entitled *Spanning Tree Algorithm*, before changing any of the parameters.

STP Parameter Settings

To change the Protocol Parameters:

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

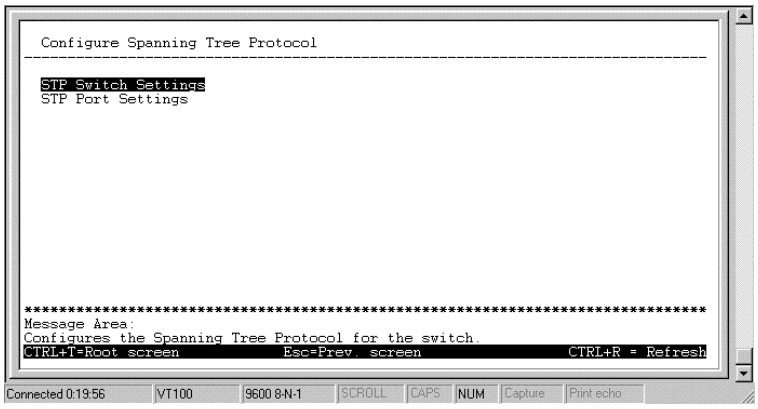


Figure 6-17. Configure Spanning Tree Protocol menu

Choose **STP Switch Settings** to access the following screen:

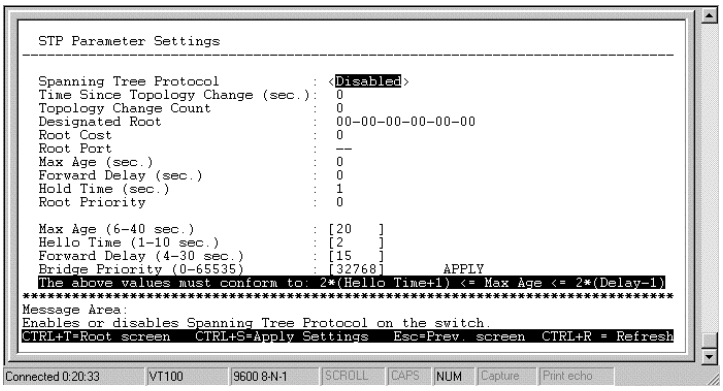


Figure 6-18. STP Parameters Setting screen

The information on the screen is described as follows:

- **Spanning Tree Protocol** Select *Enabled* to implement the Spanning Tree Protocol.
- **Time Since Topology Change(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 multi-bridged 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)** 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 multi-bridged 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.

STP Port Settings

To change the parameters on individual ports:

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

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

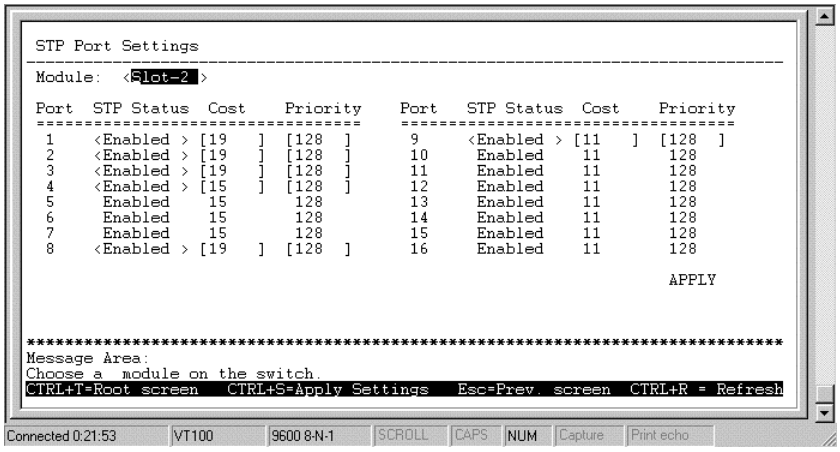


Figure 6-19. STP Port Settings screen

Items in the above window are described as follows:

- **Module** Choose a module on the switch on which to configure the Spanning Tree Port settings.
- **STP Status** Sets the Spanning Tree Protocol on a particular port to *Enabled or Disabled*.
- **Cost** The Path Cost is a read-only parameter which is the first consideration when deciding on a designated port for switch to switch connections. Each 10Mbps port has a predefined cost of 100, each 100Mbps port has a predefined cost of 19, and each 1000Mbps port has a predefined cost of 4. Trunked ports have a cost of (base cost) minus (no. of ports in the group).
- **Priority** Port Priority is a read-write object that can be set from 0 to 255. The priority is used to determine the designated port if the Path costs of redundant switch to switch connections are the same. The higher the port priority, the more chance the port has of becoming the designated port. Zero is the highest priority.

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

Configure Filtering and Forwarding Table

When a packet hits the Switch, it 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.

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.

The **Configure Filtering and Forwarding Table** screen allows you to stop or start dynamic address learning by locking the address table, change the way the Switch looks up and stores MAC address table entries, and select an age-out time for dynamically learned MAC addresses in the forwarding table. This screen also permits you to access three additional configuration screens from the menu at the bottom of the window.

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

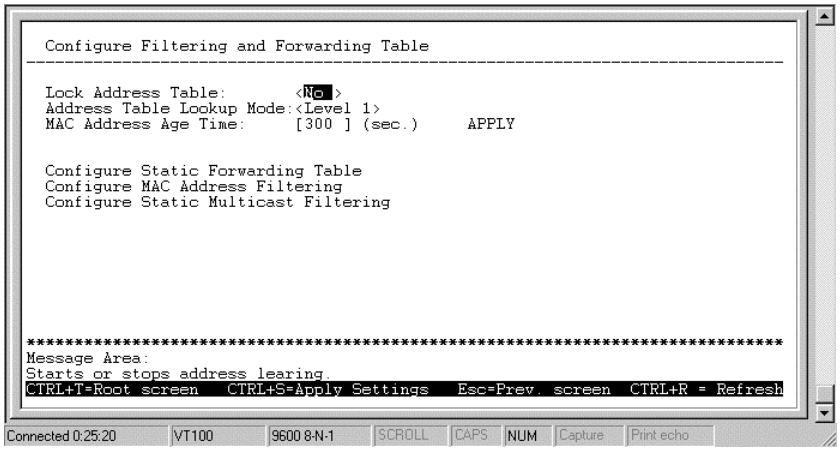


Figure 6-20. Configure Filtering and Forwarding Table screen

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

- **Lock Address Table** Mostly used 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 destined for an unknown MAC 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 Time** Enter the desired MAC address age-out time in this field (10 to 9999 seconds).

Please refer to the Packet Forwarding section of the "*Switch Management Concepts*" chapter of this manual for more detailed information.

Configure Static Forwarding Table

The Static Forwarding Table displays a list of manually defined static MAC address entries. When the Switch receives a packet with a specified MAC address in its destination field, it will always forward the packet to the specified port. These entries will never age-out.

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

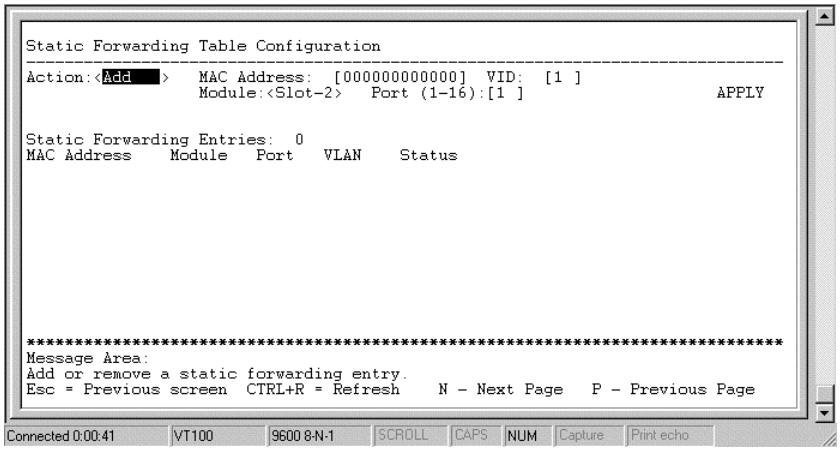


Figure 6-21. Static Forwarding Table Configuration screen

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

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

- **Action** Choose *Add* or *Remove* for each entry from the table.
- **MAC Address** Enter a MAC address in this field at the top of the screen. This is the MAC address of the device that you are creating a permanent forwarding address for. A total of ten destination addresses per page will be seen at the bottom of the screen. The Switch can hold up to 256 entries.
- **VID** This setting only appears when Port-based or 802.1Q VLANs are active and defines the VLAN ID number in the packet. Make sure the port can accept packets on this VLAN by assigning the port this VID number.
- **Module** & **Port** The module and port number are entered in these fields. The Switch will always forward traffic with the specified MAC Address and VLAN ID (if Port-based or 802.1Q VLANs are enabled) through this port.
- **Status** This is a read-only field listing the status of the static forwarding table entry. It can be "in use" or "not apply." "Not apply" means that there is a static filter for the same MAC address. Static filters always take precedence over static forwarding entries. The Switch will automatically upgrade the Status to "in use" once the static filter is removed.

Configure MAC Address Filtering

The Static Filtering Table contains filtering information configured into the Switch by (local or network) management specifying MAC addresses which are not allowed to be forwarded. The Switch will check both the destination and source MAC addresses on all packets.

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

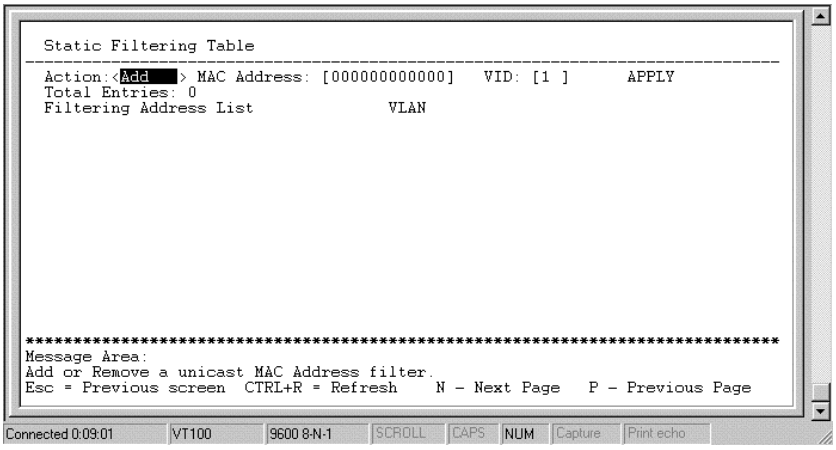


Figure 6-22. Static Filtering Table screen

To make a change to the **Static Filtering Table**, choose *Add* or *Remove* in the **Action** field. Then enter the **MAC Address** and **VID** (if Port-based or 802.1Q VLANs are enabled) and then press APPLY.

Configure Static Multicast Filtering

Multicast filtering allows you to block or forward traffic over each port for one multicast group.

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

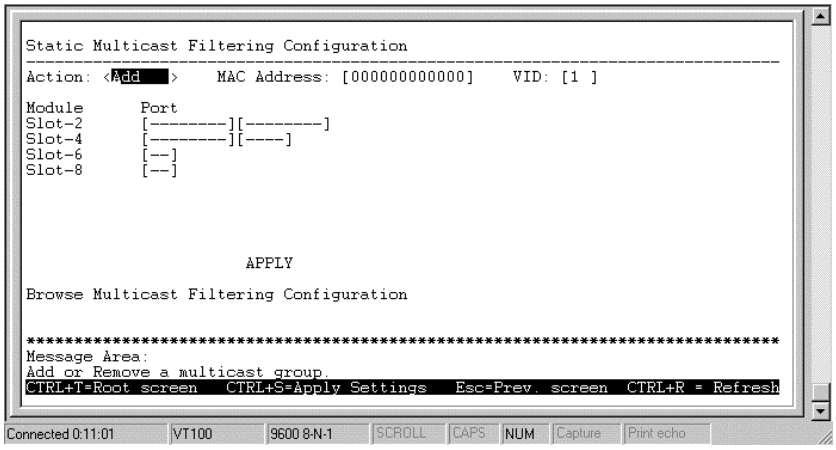


Figure 6-23. Static Multicast Filtering Configuration screen

To add or remove Static Multicast Filters, choose *Add* or *Remove* in the Action field. Then enter the multicast MAC Address and VID (if Port-based or 802.1Q VLANs are enabled). Next, choose which ports can receive packets from the multicast group by positioning the cursor over the appropriate port and hitting <space bar> to change the dash (-) to a *V*. Press APPLY to put the changes into effect.

Configure IGMP

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. Enabling IP Multicast Filtering automatically enables IGMP snooping, which enables the switch to read

IGMP packets being forwarded through the switch in order to obtain forwarding information from them (dynamically learn which ports contain Multicast members), and forward multicast packets only to the members.

Basically, in these submenus you define whether the Switch can intelligently forward IGMP packets, and you must also define which 802.1Q VLANs (if present) can send and receive IGMP and Multicast packets.

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

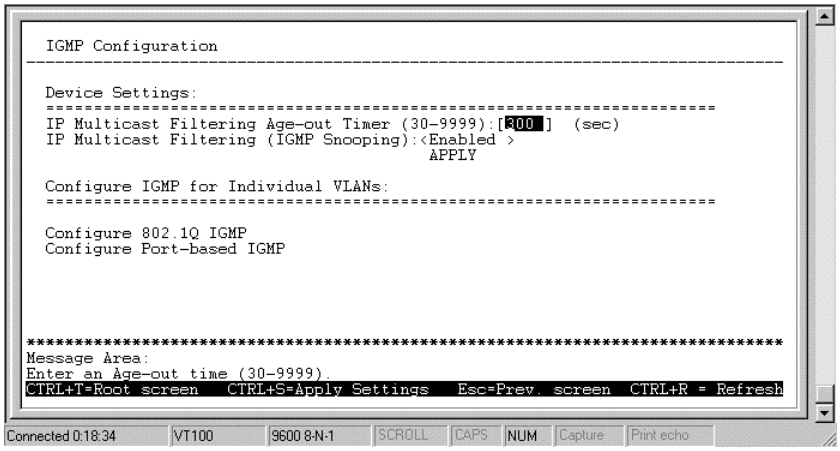


Figure 6-24. IGMP Configuration screen

Items in the above window 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).

The bottom of this screen allows you to configure IGMP for individual VLANs. If 802.1Q or port-based VLANs are enabled on your network, you must specify which VLANs can support multicast traffic. Choose **Configure 802.1Q IGMP** or **Configure Port-based IGMP** depending on the type of VLANs you are using.

802.1Q IGMP

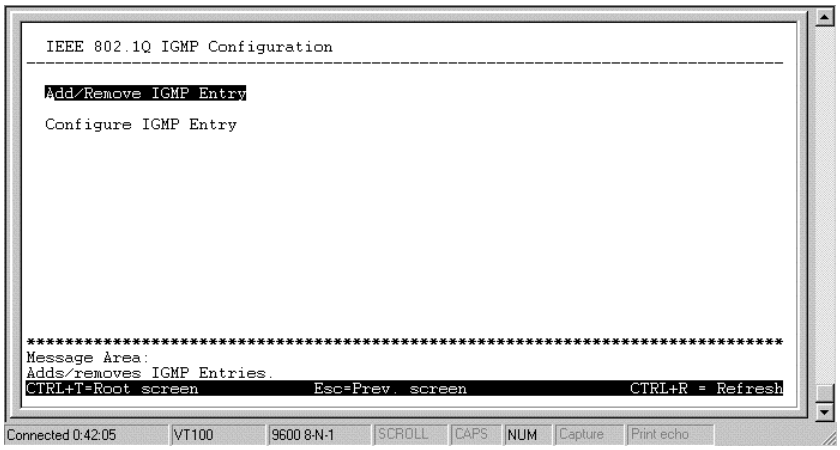


Figure 6-25. IEEE 802.1Q IGMP Configuration screen

Choose **Add/Remove IGMP Entry** from the screen above to define up to 24 VLANs on the Switch which can send and receive IGMP packets:

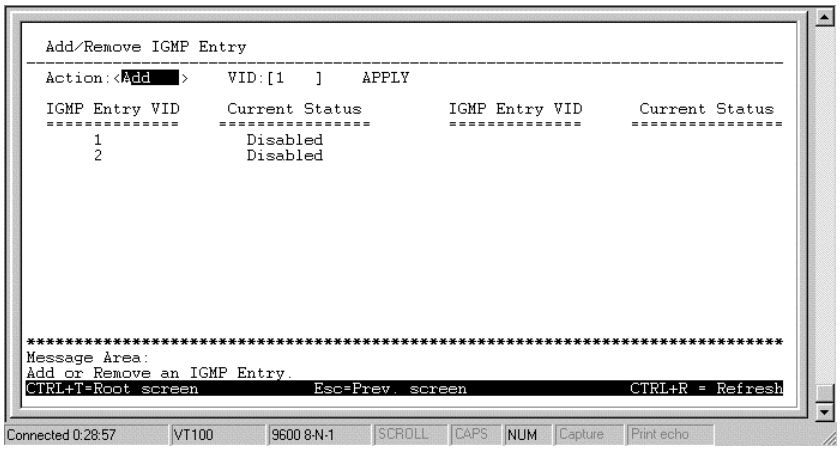


Figure 6-26. Add/Remove IGMP Entry screen

The above window is used to specify an agent to interface between IGMP and VLAN. The agents are assigned to a VLAN and allow IGMP query and report packets to be present on the given VLAN. Only 24 agents can exist on the switch at any one time.

Items in the above window are described below:

- **Action** Adds/Removes an entry (agent) from the table.
- **VID** The VLAN number that you wish to create an agent for.
- **Apply** Adds the agent to the table.

Go back to the **IEEE 802.1q IGMP Configuration** menu and choose **Configure IGMP Entry** in order to activate/deactivate the agents and configure settings for them.

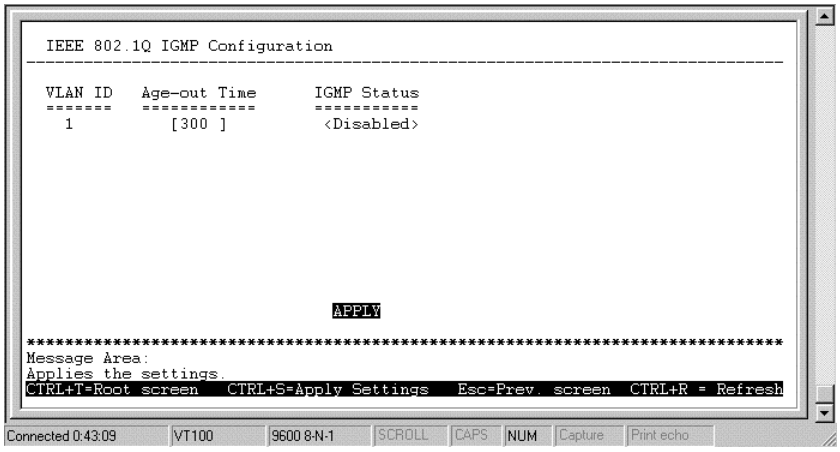


Figure 6-27. IEEE 802.1Q IGMP Configuration screen

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

Items in the above window are defined as follows:

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

Port-based IGMP

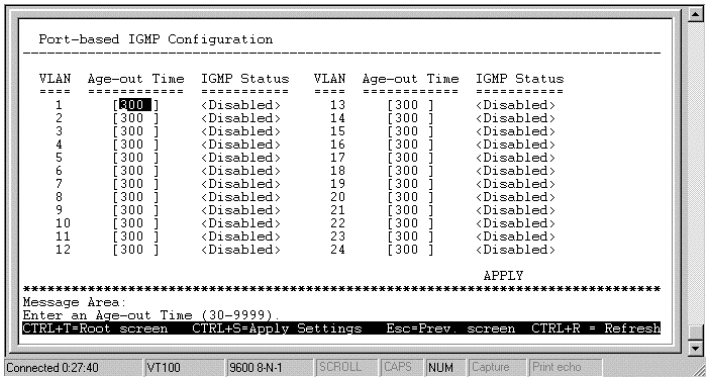


Figure 6-28. Port-based IGMP Configuration screen

This allows you to enable/disable IGMP agents for each VLAN and set aging timers for them. You can access this screen from the IGMP Configuration Screen.

Configure VLANs & MAC-based Broadcast Domains

If you are unsure about your knowledge of VLANs and MAC-based broadcast domains, please review the *VLANs & MAC-based Broadcast Domains* section in the "*Switch Management Concepts*" chapter of this manual before configuring the switch for VLANs.

The **VLANs & MAC-based Broadcast Domains Configuration** menu displays the status of the current VLAN mode and allows a user to restart the switch in a particular VLAN mode--either *Port-based*, *802.1Q*, *MAC-based* (broadcast domains) or disable VLANs on the Switch. Please note that the Switch can only support one mode at any given time. You can also access three additional screens, **Configure MAC-Based Broadcast Domains**, **Configure 802.1Q VLANs**, and **Configure Port-based VLANs**.

Choose **Configure VLANs & MAC-based Broadcast Domains Configuration** on the **System Configuration** menu to access the following screen:

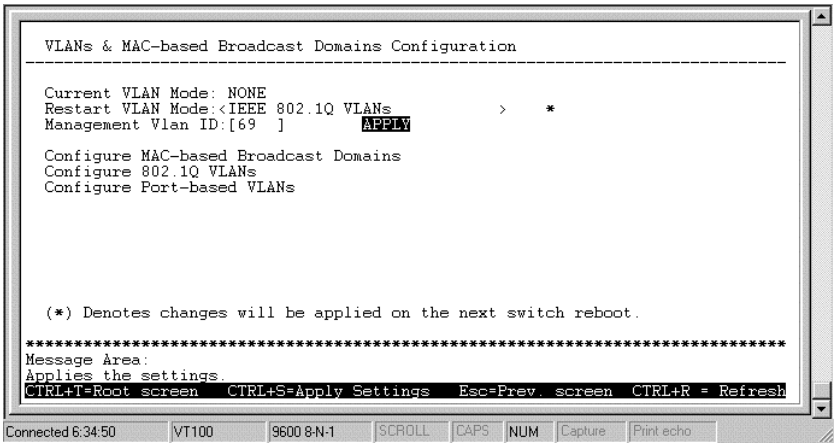


Figure 6-29. VLANs & MAC-based Broadcast Domains Configuration screen

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

- **Current VLAN Mode** Displays which type of VLAN or broadcast domain is currently enabled on the Switch.
- **Restart VLAN Mode** Choose from four settings for this mode: *Disabled, MAC-based (broadcast domain), Port-based* or *802.1Q*. After being restarted, the Switch will implement the type of VLAN or broadcast domain chosen here.
- **Management VID** When *Port-based* or *802.1Q VLANs* are enabled, this is the VLAN that will be used for management packets. Make sure the switch port that the management station is connected to has this PVID number and is a member of this VLAN (has the same VID). This should be the first VLAN you create, otherwise, you may not be able to communicate with the switch except through the console port. This setting can only be configured through the console connection. Web, Telnet and MIB management stations can only view this setting as a read-only object.

Configure MAC-Based Broadcast Domains

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

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

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

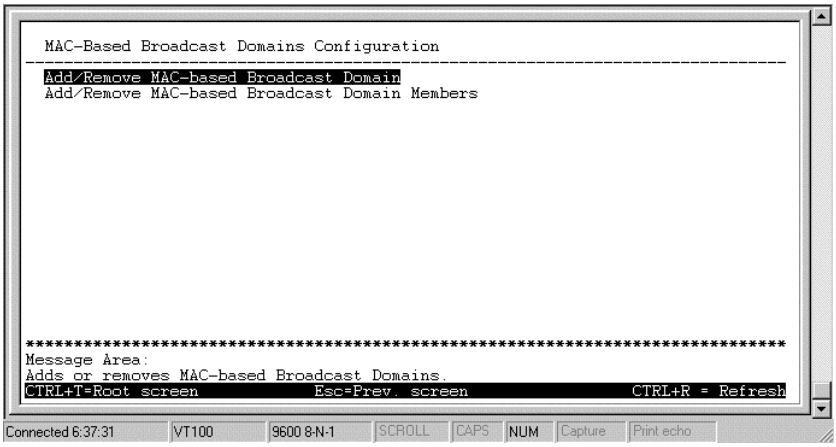


Figure 6-30. MAC-Based Broadcast Domain Configuration menu

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

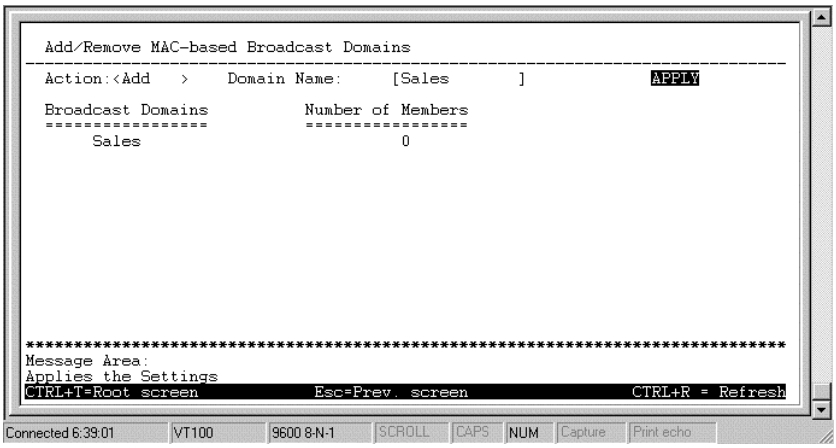


Figure 6-31. Add/Remove a MAC-based Broadcast Domain screen

The fields you can set are:

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

Press APPLY to create/remove the designated MAC-based Broadcast Domain.

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

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

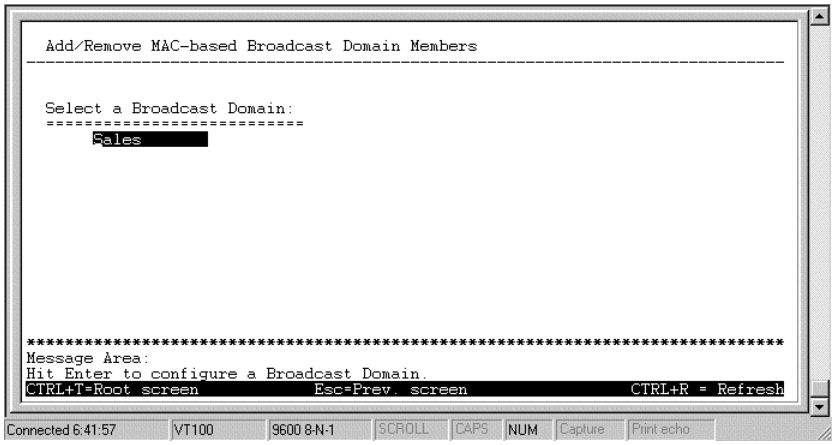


Figure 6-32. Add/Remove MAC-based Broadcast Domain Members screen

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

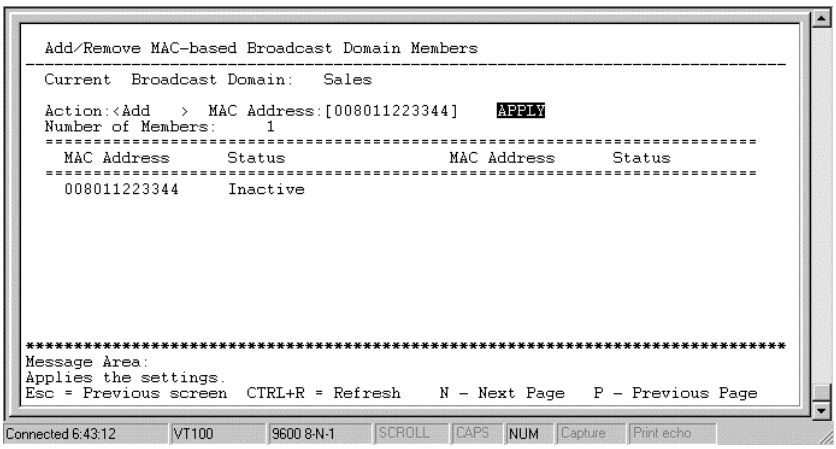


Figure 6-33. Add/Remove MAC-based Broadcast Domain Members screen

The fields you can set are:

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

Please note that the Status field for the MAC address you have entered may read Inactive. Once the Switch is restarted in MAC-based broadcast domain mode, the MAC-addresses will be applied, meaning that the broadcast domains and their entries are active.

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

Configure 802.1Q VLAN

If you are unsure of your knowledge of 802.1Q VLANs or IEEE 802.1Q tagging, we highly recommend reviewing the *VLANs & MAC_based Broadcast Domains* section of the *"Switch Management Concepts"* chapter in this manual before proceeding.

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

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

2. Define which ports will be active members of the VLAN. A port can transmit packets (coming from the connected segment) onto only one VLAN. It can receive packets (transmit packets to the connected segment) on many VLANs. Active VLAN designations are defined by assigning Port VLAN ID numbers (PVIDs) in the **Configure Default Port VLAN ID** screen. All ports participating in VLANs must have a PVID.

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

Choose **Configure 802.1Q VLANs** on the **VLAN Configuration** screen (under **Configure VLAN** of the **System Configuration** menu) to access the **802.1Q VLAN Configuration** menu:

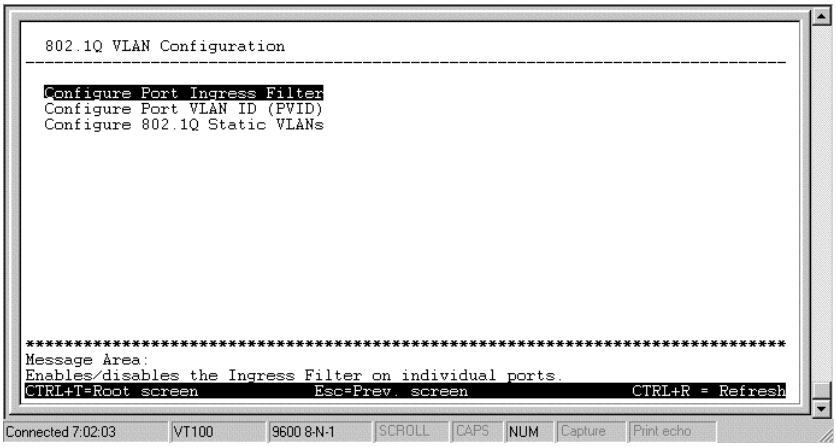


Figure 6-34. 802.1Q VLAN Configuration menu

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

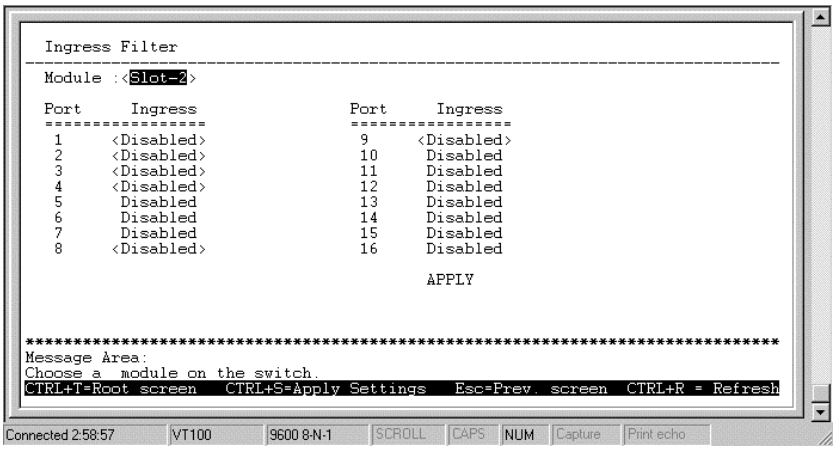


Figure 6-35. Ingress Filter screen

This screen allows you to *Enable* or *Disable* Ingress filtering for each port. When a packet arrives at the port from the connected segment and Ingress filtering is *Enabled*, the port will check the VLAN ID number of the

packet, and its own VID. If there is a match, the port will receive the packet for forwarding. If the packet doesn't have a VLAN tag or the port is not a member of the VLAN (doesn't have the same VID) as the packet, the packet will be discarded.

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

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

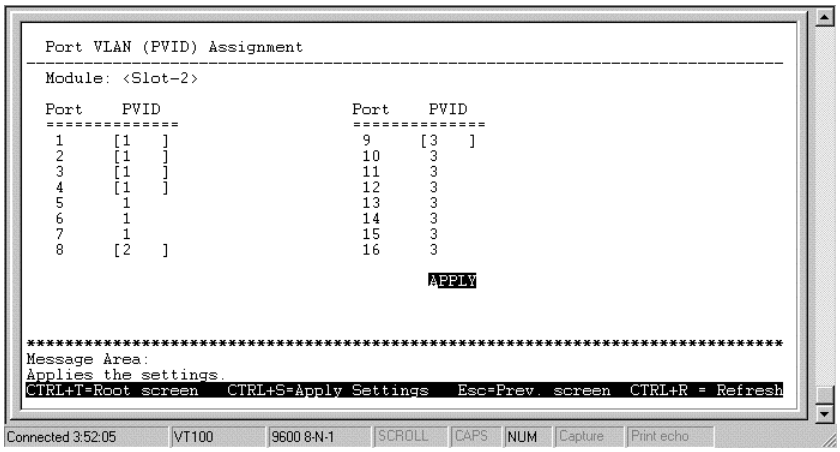


Figure 6-36. Port VLAN (PVID) Assignment screen

This screen allows you to set a Port VLAN ID number (PVID) for each port. VLAN 1 is the default VLAN. All ports are assigned PVID = 1 when VLANs are enabled. Press APPLY to let the changes take effect.

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

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

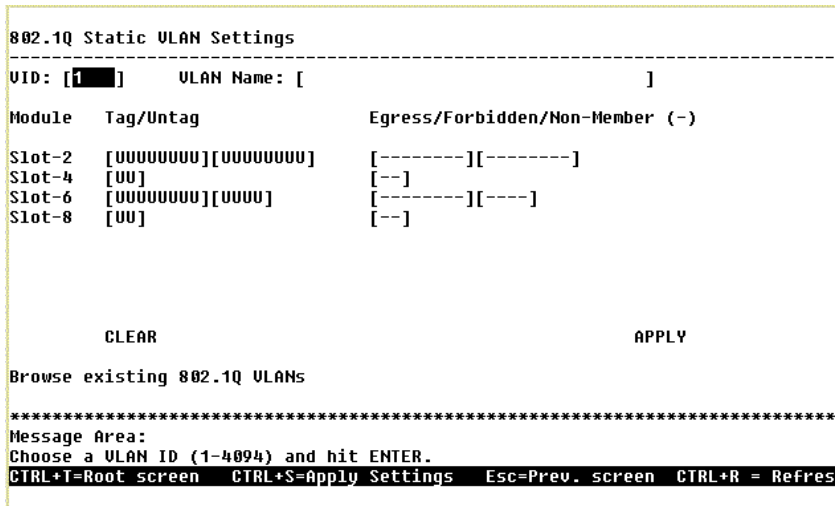


Figure 6-37. 802.1Q Static VLAN Settings screen

The fields you can set are:

- **VID** Enter a VLAN ID from 1 to 4094. This is the VLAN that will be defined on this screen. VID 1 is the default VLAN. All ports are designated members of VID 1 when VLANs are enabled.
- **VLAN Name** Description of the VLAN.
- **Tag/Untag** Toggle between *T* for Tagging Port and *U* for Untagging Port for each member port.
- **Egress/Forbidden/Non-Member** Position the cursor over the dash "–" representing the appropriate port number and press <space bar> to select *E* for Egress, *F* for Forbidden or leave the dash "–". An *E* designates the specified port as a static member of the VLAN. An *F* defines the port as a non-member and also forbids the port from joining a VLAN dynamically. A dash (–) means the port is not given VLAN membership for the VID entered above.
- **Clear** Erases the VLAN name and deselects any Egress or Forbidden settings.

Choose **Browse 802.1Q VLANs** at the bottom of the **802.1Q Static VLAN Settings** screen to access the following screen:

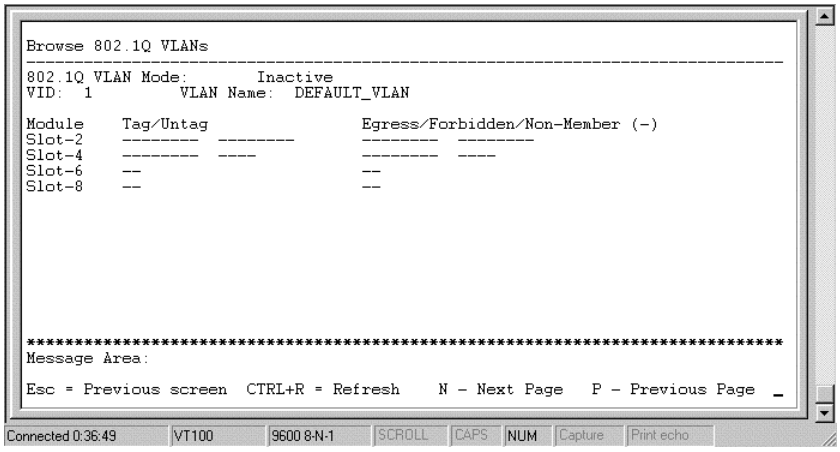


Figure 6-38. Browse 802.1Q VLANs screen

This table displays the current VID number and VLAN Name as well as Tag/Untag and Egress (membership) status for all 802.1Q static VLAN entries. Use the N key to move to the next page and the P key to move to the previous page.

Configure Port-based VLANs

Choose **Configure Port-based VLANs** to access the third item on the **VLANs & MAC-based Broadcast Domains Configuration** menu. The following screen appears:

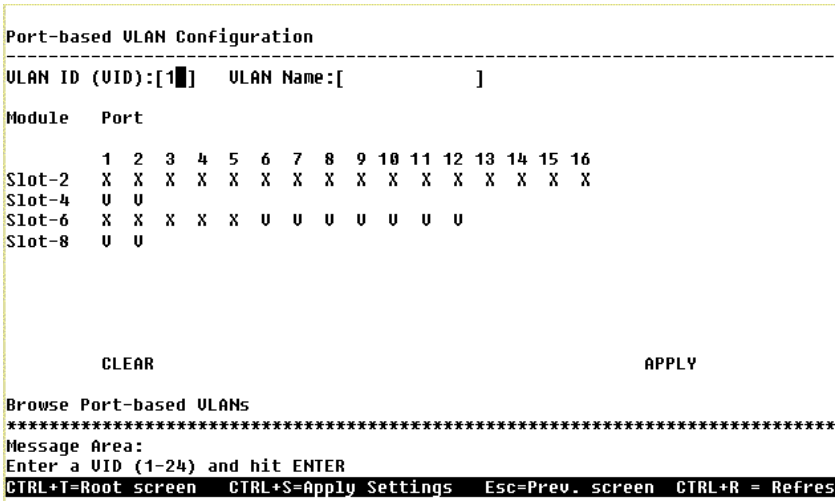


Figure 6-39. Port-based VLAN Configuration screen

The fields you can set are:

- **VLAN ID (VID)** Enter a VLAN ID from 1 to 24. This is the VLAN that will be defined on this screen. VID 1 is the default VLAN. All ports are designated members of VID 1 when VLANs are enabled. When a port is assigned to another VLAN, it is removed from VLAN 1. If it is ever removed from the other VLAN, it will automatically return to being a member of VLAN 1. Thus, all unassigned ports are automatically members of VLAN 1.
- **VLAN Name** Description of the VLAN.
- **Port Assignments** Position the cursor over the dash "–" representing the appropriate port number and press <space bar> to select "*V*" for member. Pressing <space bar> again returns the '*V*' back into a '–'. A dash (-) means the port is not given VLAN membership for the VID entered above. An 'X' shows that the port belongs to a different VLAN.
- **Clear** Erases the VLAN name and all port assignment settings.

Choose **Browse Port-based VLANs** from the screen above to view the current Port-based VLAN settings.

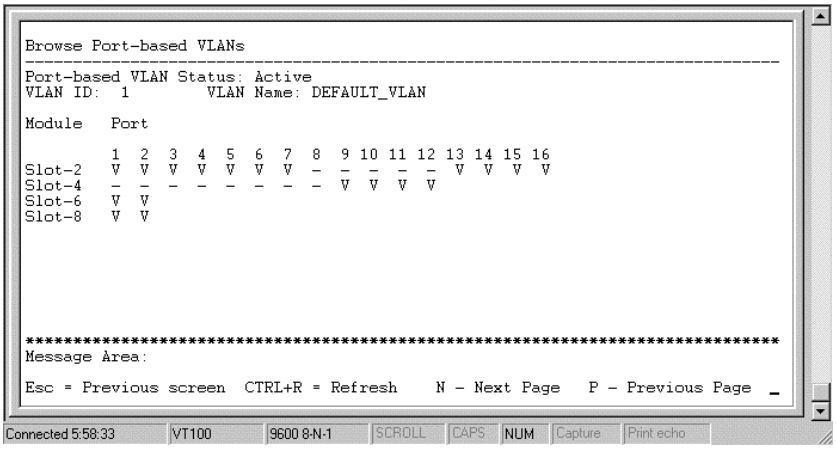


Figure 6-40. Browse Port-based VLANs screen

Update Firmware and Configuration Files

The Switch is capable of obtaining its configuration settings (the same settings defined in this console program), as well as updated versions of its internal switching software (the console program itself), using TFTP (Trivial File Transfer Protocol). You can use the **Update Firmware and Configuration Files** screen to control this feature.

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

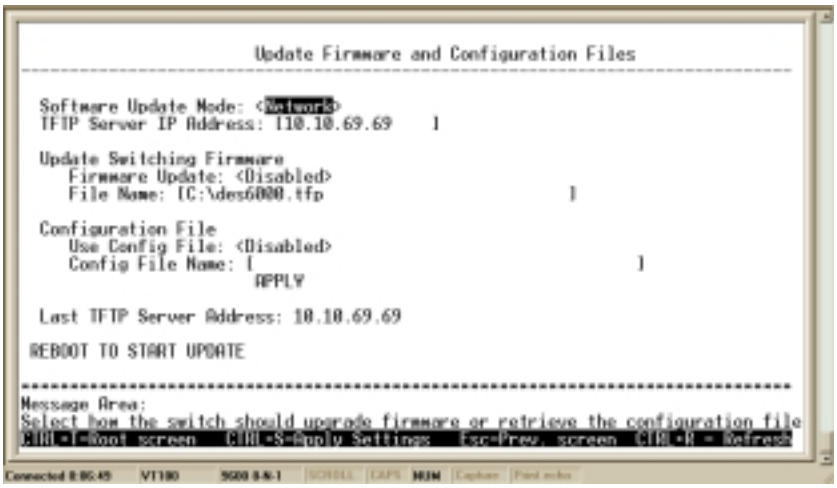


Figure 6-41. Update Firmware and Configuration Files screen

After making your changes in the fields above, press REBOOT TO START UPDATE to initiate the update sequence.

The fields you can set are:

- **Software Update Mode** Set to either *Network* or *SLIP*. Determines whether the configuration file should be obtained from a TFTP server on the Ethernet network or through the console port.
- **TFTP Server IP Address** The IP address of the TFTP server where the runtime (switching software) or configuration file is located. This entry is used only if the Firmware Update is set to *Enabled*, and the Software Update Mode is set to *Network*.
- **Firmware Update** Determines whether or not the Switch will try to look for a runtime image file on the TFTP server.
- **File Name** The complete path and filename of the runtime image file on your TFTP server to be uploaded to the Switch.
- **Use Config File** Toggle to *Enabled* to use a configuration text file when the switch is reset (rebooted). Determines whether or not the Switch should retrieve settings from a configuration file the next time it is booted.
- **Config File Name** The complete path and filename on the TFTP server for the configuration file to use. The configuration file is a text file containing IP settings for the switch. Please refer to the Sample Configuration File appendix at the back of this manual for more information on creating a configuration file.

Last TFTP Server Address is a read-only field that displays the IP address of the last TFTP server to be accessed.

For successful updates, make sure the switch can make an IP connection to the TFTP server, meaning that it is either on the same IP subnet or has a proper Gateway IP setting.

Special Notes Concerning Firmware Updates

1. Never download new firmware through a trunked port. Doing so may result in a failed download, broadcast storm, or other network problems.
2. Avoid changing active links and do not make new loops on the network when downloading new firmware.
3. Downloading new firmware may result in the loss of some or all Switch settings. We therefore strongly recommend performing a factory reset and then restarting the Switch after a successful firmware download.
4. Since new management options may be available in the updated version of the firmware, you may be unable to successfully load settings from an old settings file.

System Utilities

The **Utilities** menu offers three system utility options, **Ping Test, Upload Configuration File**, and **Upload Switch History File**.

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

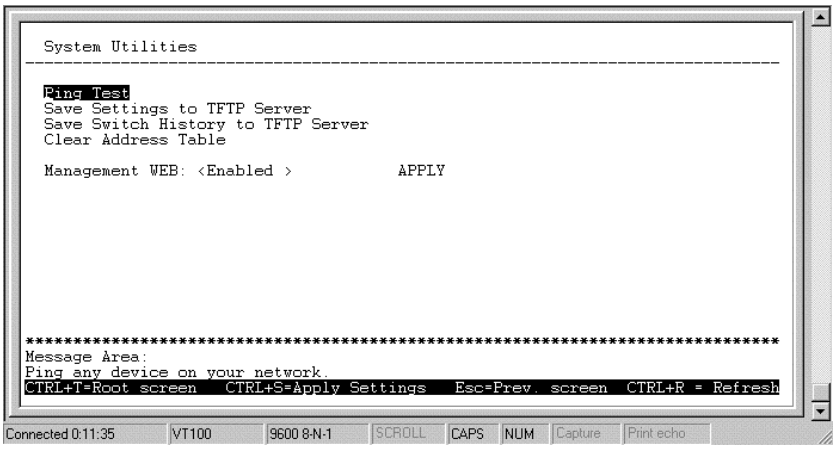


Figure 6-42. Utilities menu

Ping Test

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

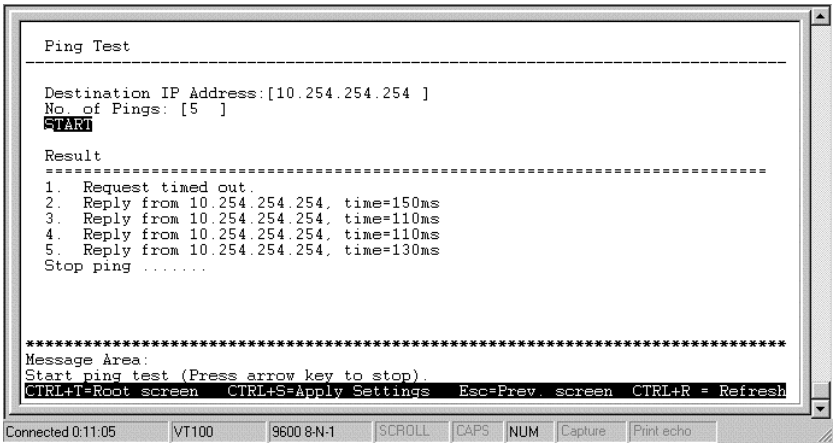


Figure 6-43. Ping Test screen

After filling in the fields above, press START to initiate the Ping test.

The fields you can set are:

- **Destination IP Address** The IP address of the device to be Pinged.
- **No. of Pings** Number 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 Results of the Ping test.

Save Settings to TFTP Server

Choose **Save Settings to TFTP Server** from the **Utilities** menu (under **System Utilities** on the main menu) to access the following screen:

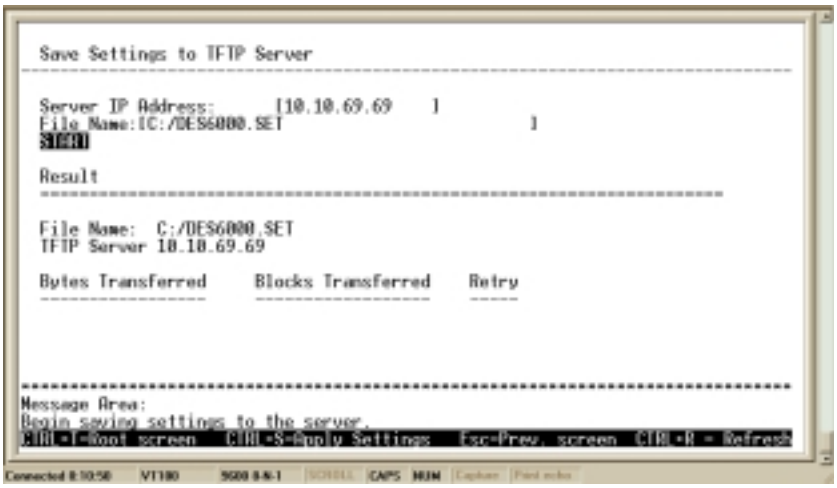


Figure 6-44. Save Settings to TFTP Server screen

Press START to begin the upload. The result will be displayed in the lower part of the screen.

The fields you can set are:

- **Server IP Address** The IP address of the TFTP server where you wish to save the settings for the Switch.

- **Configuration File Name** The complete path and filename for the file.

Save Switch History to TFTP Server

Choose **Save Switch History to TFTP Server** from the **Utilities** menu (under **System Utilities** on the main menu) to access the following screen:

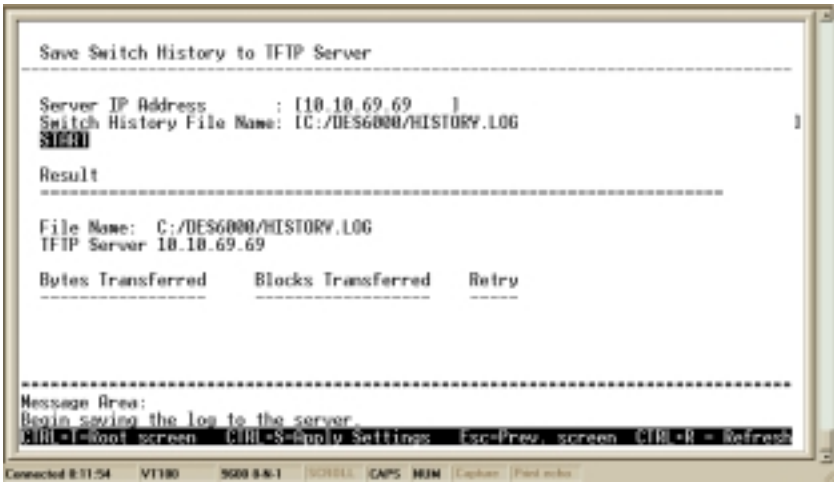


Figure 6-45. Save Switch History to TFTP Server screen

Press START to begin the file save. The result will be displayed in the lower part of the screen.

The fields you can set are:

- **Server IP Address** The IP address of the TFTP server where the switch history file will be located.
- **File Name** The complete path and filename on the TFTP server for the file.

Clear Address Table

Choose **Clear Address Table** from the **Utilities** menu (under **System Utilities** on the main menu) to clear entire MAC Address Table.

Management WEB

Allows Web-Based Network Management function to be enabled or disabled.

Community Strings and Trap Stations

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

For a detailed list of trap types used for this Switch, see the *Traps* section in the "*Switch Management Concepts*" chapter.

SNMP (version 1) implements a rudimentary form of security by requiring that each request includes 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 **Community Strings and Trap Stations** to access the third item on the main menu. The following screen appears:

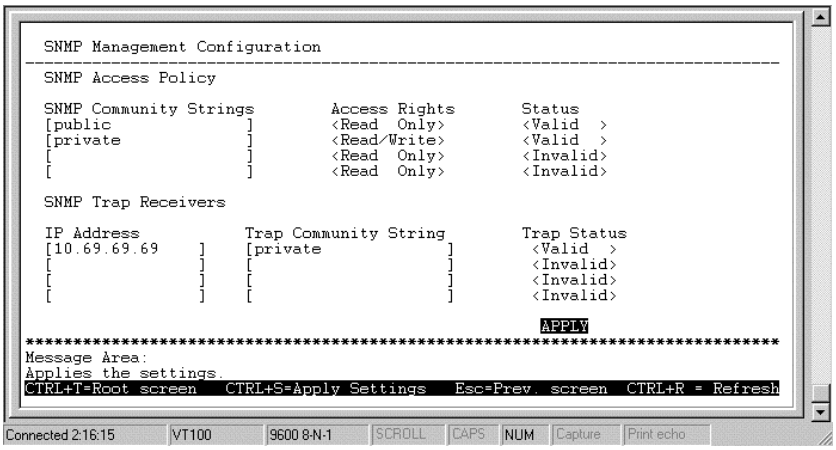


Figure 6-46. SNMP Manager Configuration screen

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

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

Switch Monitoring

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

Network Monitoring and Device Information

The **Network Monitoring and Device Information** menu offers five items, **Traffic Statistics**, **Browse Address Table**, **Switch History**, **Browse IGMP Status** and **Device Status**.

Choose **Network Monitoring and Device Information** from the main menu. The following menu appears:

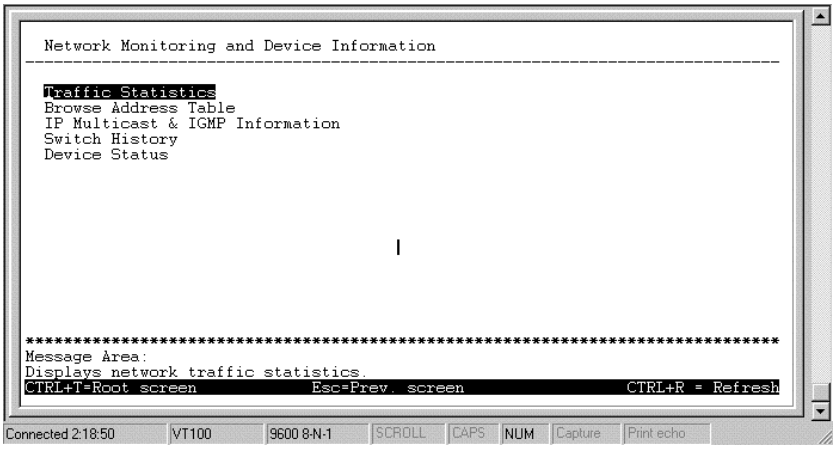


Figure 6-47. Network Monitoring and Device Information menu

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

Traffic Statistics

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

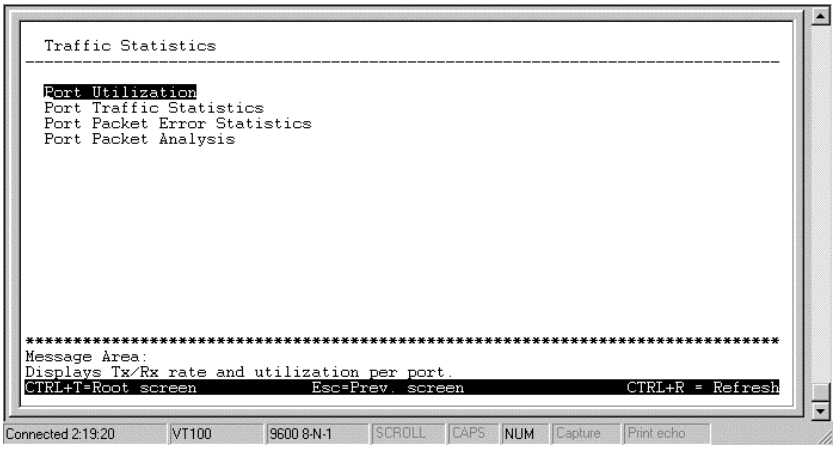


Figure 6-48. Traffic Statistics menu

Port Utilization

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

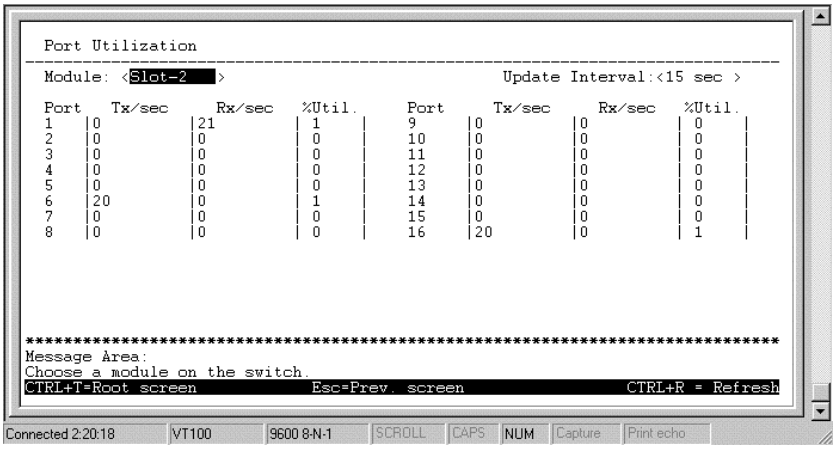


Figure 6-49. Port Utilization screen

Select the desired device in the Switch field and the desired increment setting in the Update Interval field: *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.

The statistic counters displayed are defined as follows:

- **Update Interval** *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*. The setting causes the switch to sample the wire at the interval chosen.
- **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 during a single second at the time specified by the update interval. The utilization percentage is the total number of bits transmitted and received on the port per second divided by the bandwidth per second. Please note that bandwidth values are doubled for full-duplex connections (i.e. 100BASE-TX at full duplex is 200Mbps).

Port Traffic Statistics

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

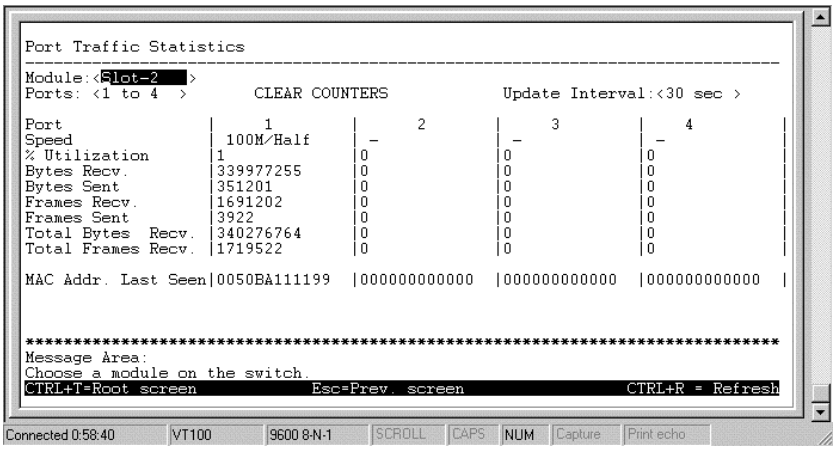


Figure 6-50. Port Traffic Statistics screen

Select the desired module in the Module field, the desired port range in the Ports field, and the desired increment setting in the Update Interval field: *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.

The statistic counters displayed are defined as follows:

- **Speed** If the link is up, the speed and duplex status will be displayed; if the link is down "-" will be displayed.
- **% Utilization** This shows the percentage of available bandwidth each port is using during a single second at the time specified by the update interval. The utilization percentage is the total number of bits transmitted and received on the port per second divided by the bandwidth per second. Please note that bandwidth values are doubled for full-duplex connections (i.e. 100BASE-TX at full duplex is 200Mbps).
- **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 last device that sent packets over this port.

Port Packet Error Statistics

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

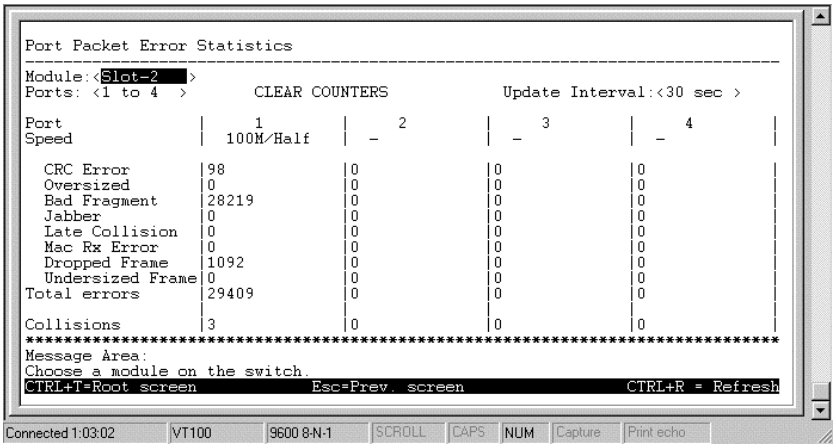


Figure 6-51. Port Packet Error Statistics table

Select the desired device in the Switch field, the desired setting in the Ports field, and the desired increment setting in the Update Interval field: *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.

The statistic counters displayed are defined as follows:

- **Speed** If the link is up, the speed and duplex status will be displayed; if the link is down "-" will be displayed.
- **CRC Error** The number of frames that fail the CRC integrity check.
- **Oversize** The number of good frames with length greater than 1536 bytes and therefore are greater than the maximum legal length.

- **Bad Fragment** The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
- **Jabber** The number of frames with length more than 1536 bytes and with CRC error or misalignment (bad framing).
- **Late Collision** The number of collisions that occur at or after the 64th byte (octet) in the frame.
- **Mac Rx Error** The number of frames with received MAC Errors.
- **Dropped Frames** The number of frames which are dropped by this port since the last Switch reboot.
- **Undersize Frames** The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
- **Total errors** The sum of the CRC Error, Oversize, Bad Fragment, Jabber, Late Collision, Mac Rx Error, Dropped Frames, and Undersize Frames counters.
- **Collisions** The number of times packets have collided on this port.

Port Packet Analysis Statistics

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

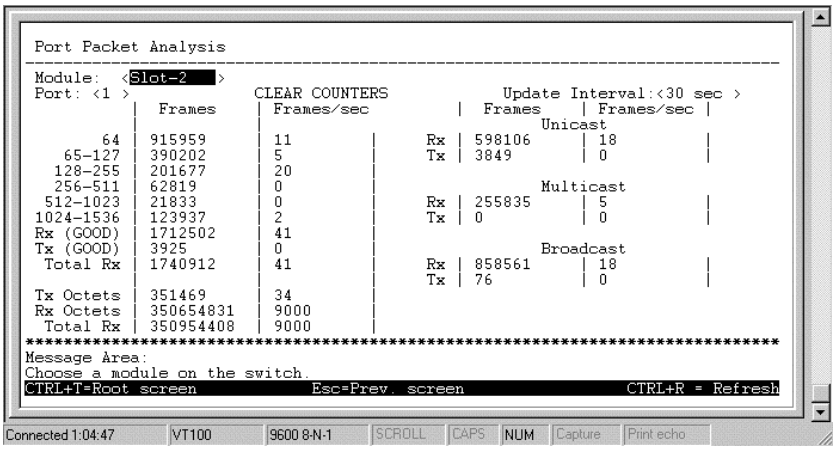


Figure 6-52. Port Packet Analysis table

Select the desired module in the Module field, the desired port in the Port field, and the desired increment setting in the Update Interval field: *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*.

The statistic counters displayed are defined as follows:

- **64**, **65-127**, **128-255**, **256-511**, **512-1023**, **1024-1536** 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.

Browse Address Table

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

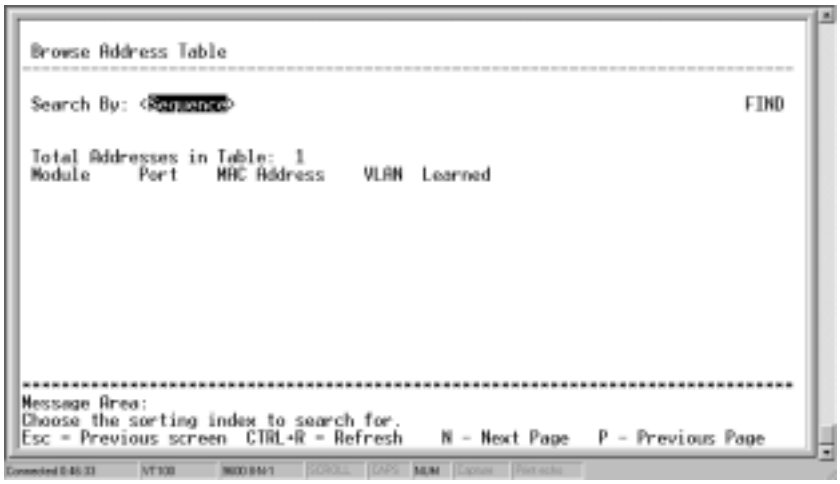


Figure 6-53. Browse Address Table

Use the space bar to select the method you wish to use to browse the address table in the Search By field. Use <Enter> or arrow keys to navigate the screen. The FIND command initiates the search.

Search options include: *Sequence*, which allows you to browse MAC addresses by numerical sequence, *MAC*, which searches for the MAC address specified in the MAC Address field (this is only displayed when *MAC* has been selected in the Search By field), and *Port*, which allows you to specify a Module and Port (these two fields only appear when *Port* has been selected in the Search By field).

The message area at the bottom of the screen will display pertinent information regarding the function of the highlighted screen command or tell you when no addresses can be found.

Switch History

The **Network Monitoring and Device Information** menu allows the user to view the Switch history. This works like a trap and event receiver except it only captures trap/events generated by the Switch itself. For example, the switch history includes when the system is rebooted, when a console session has timed-out, when a new link is established, and when configuration is saved to flash memory.

To display the **Switch History** screen, choose **Network Monitoring** from the main menu and then choose **Switch History**. The following screen appears:

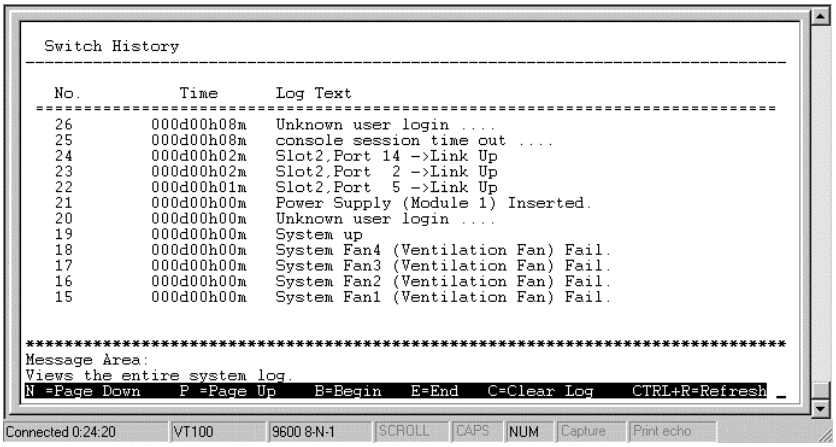


Figure 6-54. Switch History screen

The switch history entries are listed chronologically from the last time the Switch was rebooted.

Device Status

Selecting Device Status will display power supply and fan status. From this screen you can activate or deactivate the buzzer.

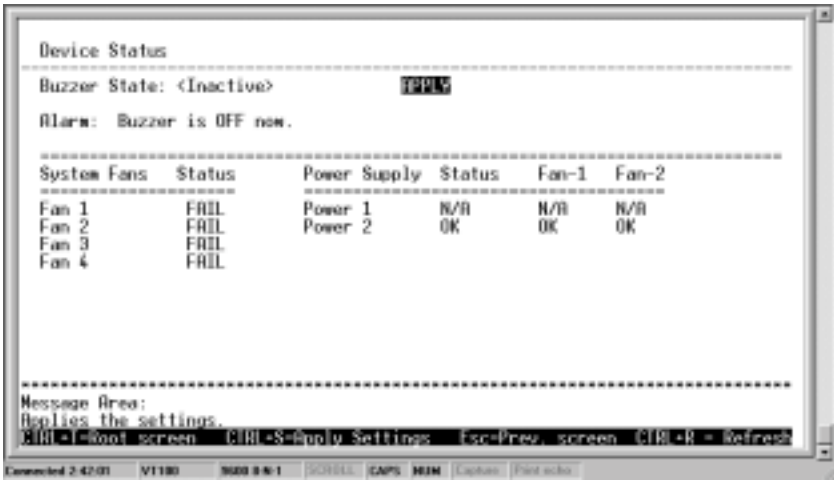


Figure 6-55. Device Status screen

IP Multicast and IGMP Information

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

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

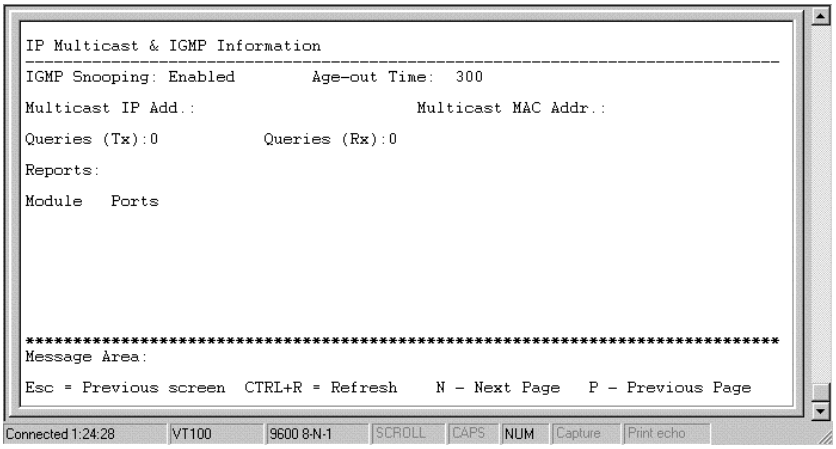


Figure 6-56. IP Multicast & IGMP Information screen

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 Time** Displays the time the Switch waits between IGMP queries.
- **VLAN** Displays the VLAN ID number.
- **Multicast IP Add.** The Multicast IP address of the Multicast group being displayed.
- **Multicast MAC Address** The Multicast MAC address of the multicast group being displayed.
- **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.
- **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.

Resetting the Switch

Switch settings may be reset simply by powering the Switch off and on again, or by performing a Restart System or Factory Reset using either the console interface or the Web-Based Network Management function discussed in Chapter 7. Some functions, such as changing or enabling VLAN settings, require that the Switch be restarted and will therefore reset the Switch.

Remember that restarting the Switch will erase all settings in RAM and reload them from the NV-RAM. Use the Save Changes function to save current switch settings (in RAM) to NV-RAM before resetting the switch (see the *Save Changes* section in this manual for more details). If you choose to restart the switch by powering the Switch off and then on, be sure to first perform a Save Changes if you wish to save any settings that have been changed. When using the Restart Switch function of the console interface or the Web-Based Network Management program you are given the option of saving any changes to settings before the Switch actually restarts.

A Factory Reset will set all of the Switch's parameters to their original settings as they were when the Switch was delivered from the factory. Please read the following section concerning Factory Reset.

Factory Reset

IMPORTANT: 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, even those 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 values present when the Switch was purchased.

After performing the Factory Reset, make sure to redefine the IP settings for the Switch in the **Configure IP Address** menu. Then perform a Restart System on the Switch. After these three procedures are performed, your Factory Reset is complete.

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

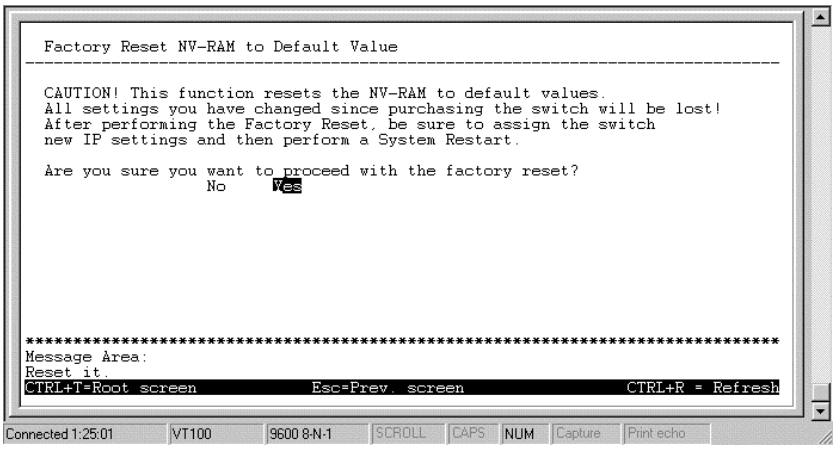


Figure 6-57. Factory Reset NV-RAM to Default Value screen

Logout

To exit the console program, choose **Logout** from the main menu. Make sure you have performed a Save Changes if you have made changes to the settings and wish them to become defaults for the switch. After logging out, you will be returned to the opening login screen.

7

WEB-BASED NETWORK MANAGEMENT

Introduction

The Switch 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 (versions 4.0 or later). 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 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).

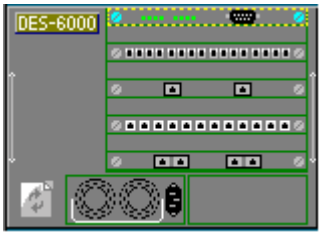
Management

To begin managing your Switch simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the switch.

In the page that opens, click on the **Login to DES-6000 Manager** button:

This opens the main page in the management module.

The top-left part of each page contains an interactive view of the Switch's front panel as shown below. The image on your browser may appear slightly different depending on the modules you have installed.



Clicking on one of the modules causes an interactive view of the front-panel of the chose module at the top of the browser. The default module displayed when you first open the page is the CPU module shown below:

Clicking on one of the ports in a networking module opens a configuration window for that particular port.

Each page contains the following list of buttons in the panel on the left side: **Configuration**, **Management,** **Monitoring,** and **Maintenance**. These are the main categories for Switch management.

The switch management features are explained below.

Configuration

This first category includes: **IP Address**, **Switch Module** (**Switch Module Information** and **Advanced Settings**), **Port**, **Trunk Groups**, **Port Mirroring**, **Spanning Tree Protocol** (**STP Switch Settings** and **STP Port Settings**), **Forwarding and Filtering** (**Static Forwarding Table**, **MAC Address Filtering Table**, and **Static Multicast Filtering**), **IGMP** (**IGMP Settings**, **802.1Q IGMP**, and **Port-based IGMP**), and **VLANs & MAC-based Broadcast Domains** (**MAC-based Broadcast Domains**, **802.1Q VLANs**, and **Port-Based VLANs**), as well as a number of related windows.

IP Address

Figure 7-1. IP Address window

You can change the IP Address, Subnet Mask, and Default Gateway on the Switch. If your are not using BOOTP, enter the IP Address, Subnet Mask, and Default Gateway of the Switch. If you enable BOOTP Service, 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 above is described as follows:

- **Switch MAC Address** The Ethernet address for the switch. Also known as the physical address.
- **Get IP from** Choose either *Manual*, where you assign them in the fields below, *BOOTP* or *DHCP*. The BootP and DHCP protocols allow IP addresses, subnet masks, and default gateways to be assigned on a central server. If this option is enabled, when the Switch is first powered up it will look for the appropriate server to provide it with these settings.
- **IP Address** The IP Address for the switch on the TCP/IP network.
- **Subnet Mask** The subnet mask that controls subnetting on your TCP/IP network.
- **Default Gateway** The IP address of the device, usually a router, that handles connections to other subnets and/or other TCP/IP networks.

Switch Module

The **Switch Module** screen shows various pieces of information about your Switch, and allows you to set the System Name, System Location, and System Contact.

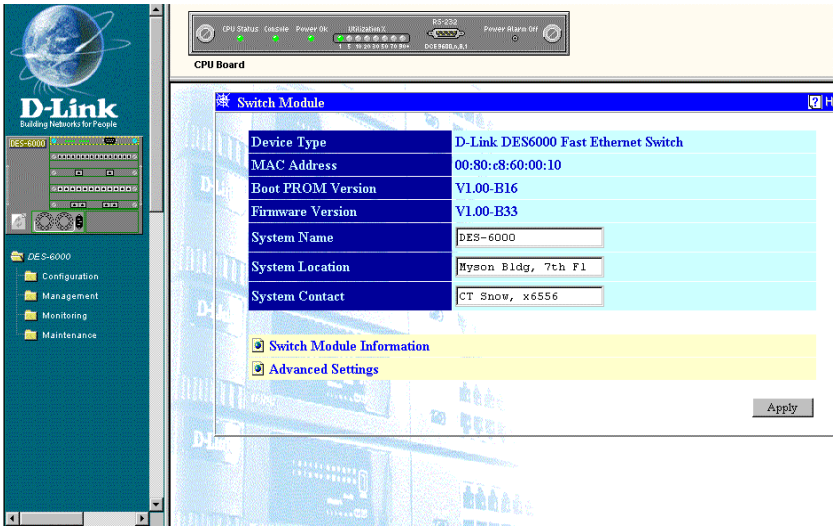


Figure 7-2. Switch Module window

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.

Switch Module Information

The **Switch Module Information** window lists the type of modules currently installed in the switch.

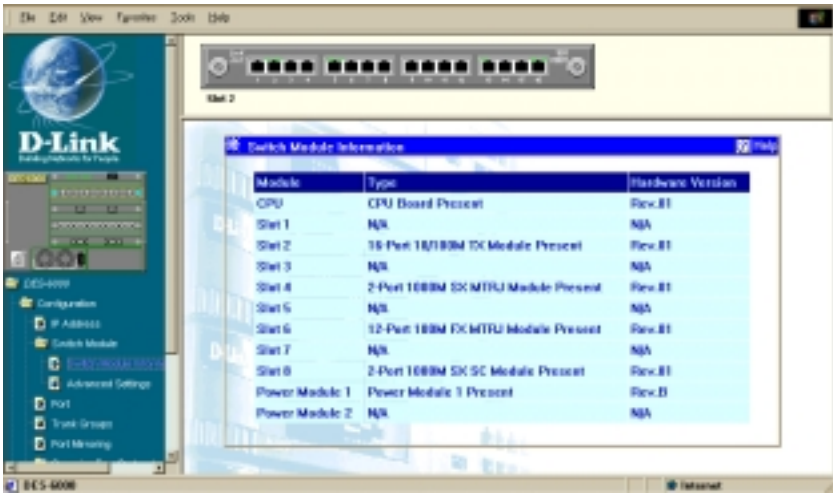


Figure 7-3. Switch Module Information window

Advanced Settings

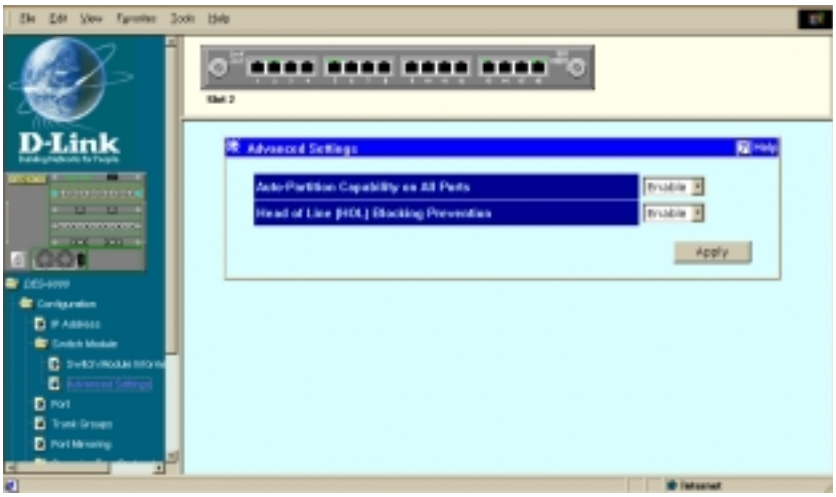


Figure 7-4. Advanced Settings window

The first setting allows you to enable or disable port auto-partitioning by the Auto-Partition Capability on All Ports function. If you enable auto-partitioning on all ports, when more than 62 collisions occur while a port is transmitting data, the port automatically stops transmissions. The second setting allows you to enable or disable the Head of Line (HOL) Blocking Prevention function. Click **Apply** to let your changes take effect.

The information above is described as follows:

- **Auto-Partition Capability on All Ports** This option offers *Enable* or *Disable* to decide whether to auto-partition a selected port and take it offline or not.
- **Head of Line (HOL) Blocking Prevention** Head-of Line blocking occurs when a packet originating on Port 1, for instance, needs to be forwarded to Ports 2 and 3. If Port 2 is occupied (causing the packet to be held in memory until the port is free), the packet destined for Port 3 will also be delayed, even though Port 3 may be free. Cumulatively, these delays can have a noticeable effect on overall network performance. Enabling HOL Blocking Prevention prevents Head-of-Line blocking from occurring, meaning that the packet destined for Port 3 gets delivered immediately.

Port

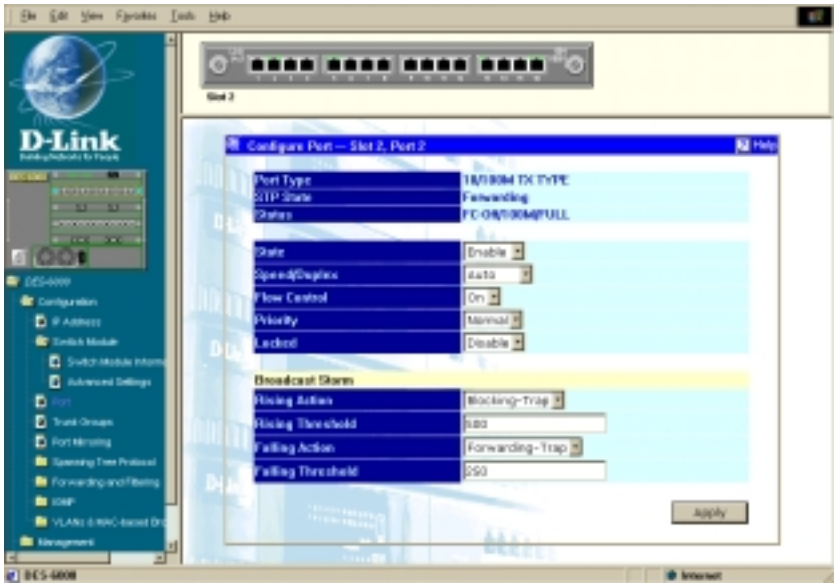


Figure 7-5. Configure Port window

Select the port you want to configure by clicking on the port in the module front panel display at the top of the screen (click on specific modules on the representation of the entire Switch to the left to make them appear at the top of the window). Follow these instructions:

1. State enables or disables the port. If you choose *Disable*, 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 **MAC Forwarding Table**.

2. Configure the **Speed/Duplex** setting for the port. Select *Auto* for Auto-Negotiation. This allows the port to select the best transmission speed and duplex mode based on the capabilities of the device at the other end. Select *100/Full* for port operation at 100 Mbps and full duplex. Select *100/Half* for port operation at 100 Mbps and half duplex. Select *10/Full* for port operation at 10 Mbps and full duplex. Select *10/Half* for port operation at 10 Mbps and half duplex. If a Gigabit Ethernet port is selected, the only option is *1000/Full*.

3. Configure the **Flow Control** setting for the port. Selecting *On* in full-duplex mode will implement IEEE 802.3x flow control. Selecting *On* when the port is in half duplex mode will implement normal Ethernet collision-based backpressure flow control. Select *Off* for no flow control. Also, if the port is set for *Auto* in the speed/duplex field above and flow control is enabled, flow control (whether full- or half-duplex) will only be implemented if the other device can auto-negotiate flow control.

4. **Priority** settings are *Normal*, *High* or *Low*. The Switch has two packet queues where incoming packets wait to be processed for forwarding; a high priority and low priority queue. The high priority queue should only be used for data in which latency can have adverse affects on the function of an application, such as video or audio data, where latency can produce distorted sounds and images. Packets in the low priority queue will not be processed unless the High priority queue is empty. Setting the port priority to *High* will deliver all packets arriving at the port to the high priority queue, a *Low* setting will send them all to the low priority queue. The *Normal* setting causes the port to examine the packet for an IEEE 802.1p/Q priority tag. If no tag exists, the packet will be sent to the low priority queue. If the priority tag field in the packet header contains a value of 0-3, the packet will be placed in the low priority queue; a value of 4-7 causes the packet to be placed in the high priority queue.

5. Configure the **Locked** setting to prevent the port from learning the MAC addresses of new hosts. This will help keep intruders off your network since any packet coming from an unknown source address will be dropped by the Switch, that is, not added to your MAC Address Forwarding Table. Select *Enable* or *Disable*.

6. Configure the **Rising Action** setting under **Broadcast Storm** from three choices: *Do-Nothing*, *Blocking*, or *Blocking-Trap*. You can also set a **Rising Threshold** in the next field. Otherwise, the default is 500 packets per second.

7. Configure the **Falling Action** setting under **Broadcast Storm** from three choices: *Do-Nothing*, *Forwarding*, or *Forwarding-Trap*. You can also set a **Falling Threshold** in the next field. Otherwise, the default is 250 packets per second.

8. The **Port Type**, **STP State**, and **Status** are read-only fields indicating the current condition of the port you have selected.

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

Trunk Groups

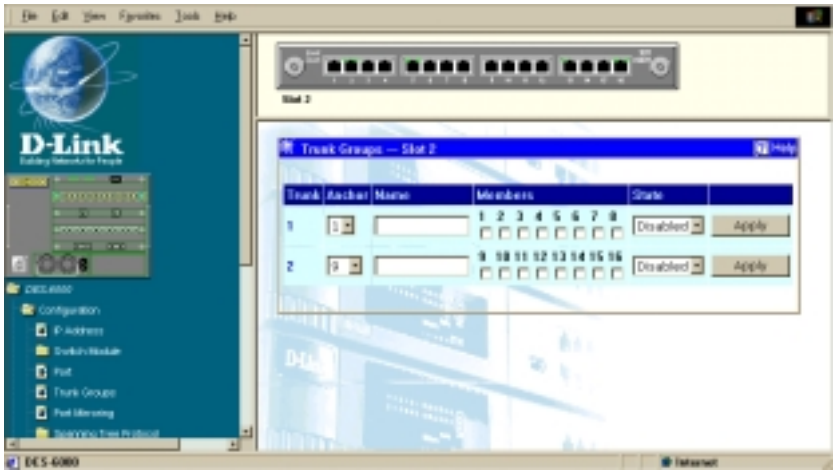


Figure 7-6. Trunk Groups window

The Switch supports up to 16 trunk groups. Each module on the Switch supports up to two trunk groups except Gigabit modules which don't support trunk groups. Trunks are groups of ports that are banded together to form a single, logical, high-bandwidth data pipe.

Items in the above window are defined as follows:

- **Anchor** The Anchor port for the trunk group. All configuration settings changes made to the anchor port will automatically be made to the other ports in the trunk.
- **Name** The user-assigned name of the trunk group.
- **Members** The continuous number of ports that will be members of the trunk group.
- **State** Allows the trunk group to be *Enabled* or *Disabled*. *Clear* the third choice, deselects all ports and erases the name of the trunk group.

Port Mirroring

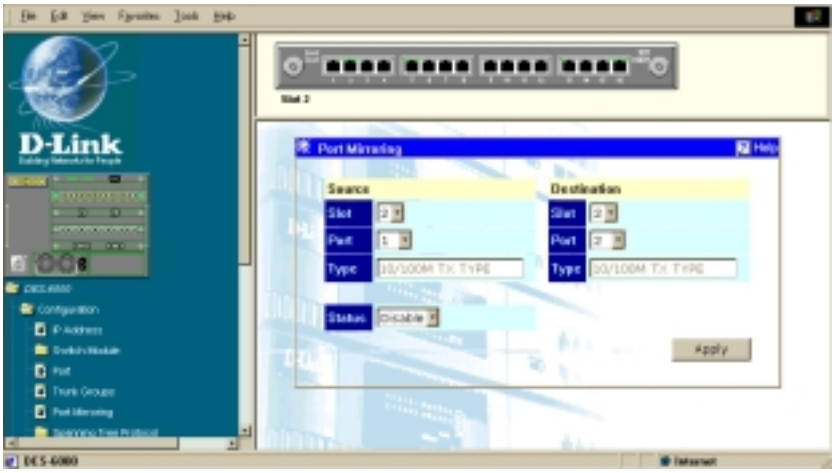


Figure 7-7. Port Mirroring window

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

To configure a mirror port, select the Slot, and source Port from where you want to copy frames in the Source section. Next, select the Slot and target Port which will receive the copies in the Destination section. The destination port is where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe. To complete the port mirroring, select *Enable* in the Status field and click **Apply**.

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

Spanning Tree Protocol

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 Concepts*" chapter for a detailed explanation.

STP Switch Settings

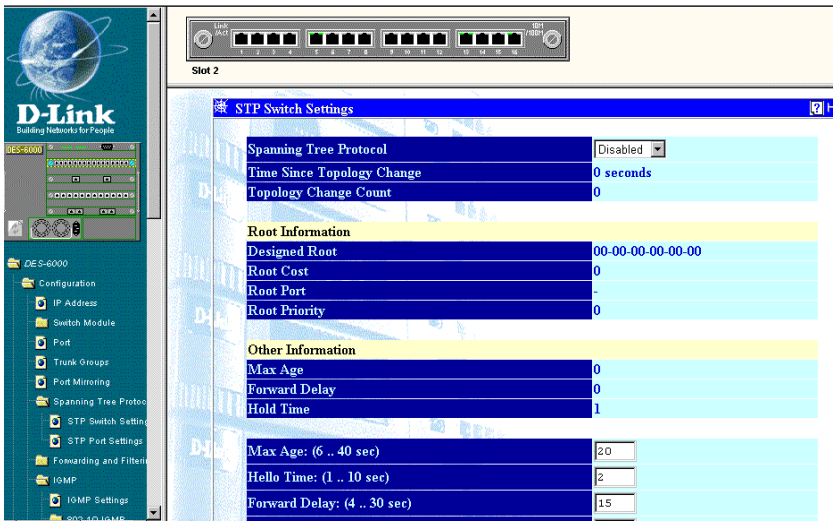


Figure 7-8. STP Switch Settings window

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

The items you can change include:

- **Spanning Tree Protocol** This option allows you to enable or disable Spanning Tree Protocol on a switch-wide basis.
- **Max Age: (6 . . 40 sec)** The Maximum Age can be from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.
- **Hello Time: (1 . . 10 sec)** 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.
- **Forward Delay: (4 . . 30 sec)** The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.
- **Bridge Priority: (0 . . 65535)** A Bridge Priority can be from 0 to 65535.

STP Port Settings

Figure 7-9. STP Port Settings window

Enter the desired Spanning Tree custom settings on this screen and then click **Apply**.

The information above is described as follows:

- **STP Status** The Spanning Tree Protocol state for a selected port can either be *Enabled* or *Disabled*.
- **Cost** The Path Cost is a read-only parameter which is the first consideration when deciding on a designated port for switch to switch connections. Each 10Mbps port has a predefined cost of 100. Each 100Mbps port has an assigned Path Cost of 19. Gigabit ports have a cost of 4. Trunked ports have a cost of (base cost) minus (no. of ports in the group).
- **Priority** Port Priority is a read-write object that can be set from 0 to 255. The priority is used to determine the designated port if the Path costs of redundant switch to switch connections are the same. The higher the port priority, the more chance the port has of becoming the designated port. Zero is the highest priority.

Forwarding and Filtering

When a packet hits the Switch, it 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.

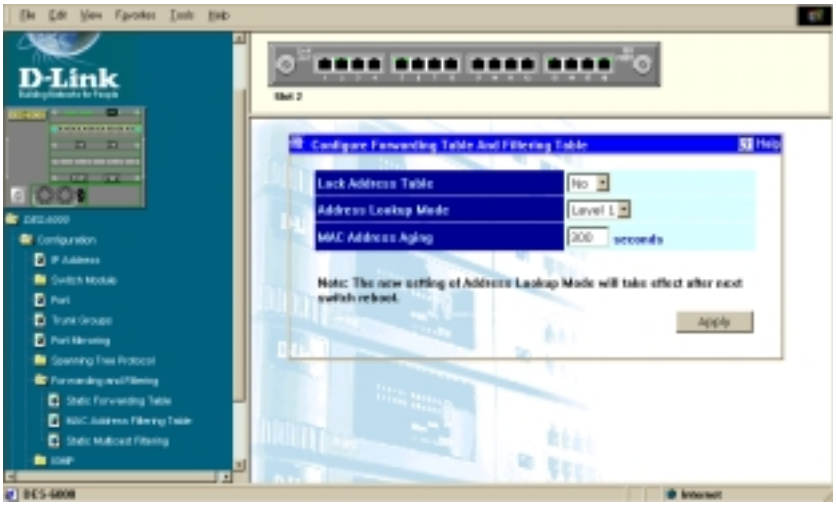


Figure 7-10. Configure Forwarding Table And Filtering Table window

This window allows you to stop or start address learning, designate an address look-up mode, and select an age-out time for MAC addresses. Click **Apply** to let your changes take effect.

The following fields above can be set:

- **Lock Address Table** Mostly used for security purposes, when the forwarding table is locked the Switch will no longer learn the MAC addresses of 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 Lookup Mode** Select from: *Level 0*, *Level 1*, *Level 2*, *Level 3*, *Level 4*, *Level 5*, *Level 6*, or *Level 7*.
- **MAC Address Aging** Enter the desired MAC address aging time in this field (10 to 9999 seconds).

Static Forwarding Table

Figure 7-11. Static Forwarding Table window

MAC forwarding allows the Switch to permanently forward outbound traffic to specific destination MAC addresses over a specified port. To use the MAC forwarding function, enter a MAC address. Whenever the Switch sees a packet with this destination MAC Address, it will forward it over the module, port, and VLAN you specify.

Click **New** to access the **Static Forwarding Table --- Edit** window:

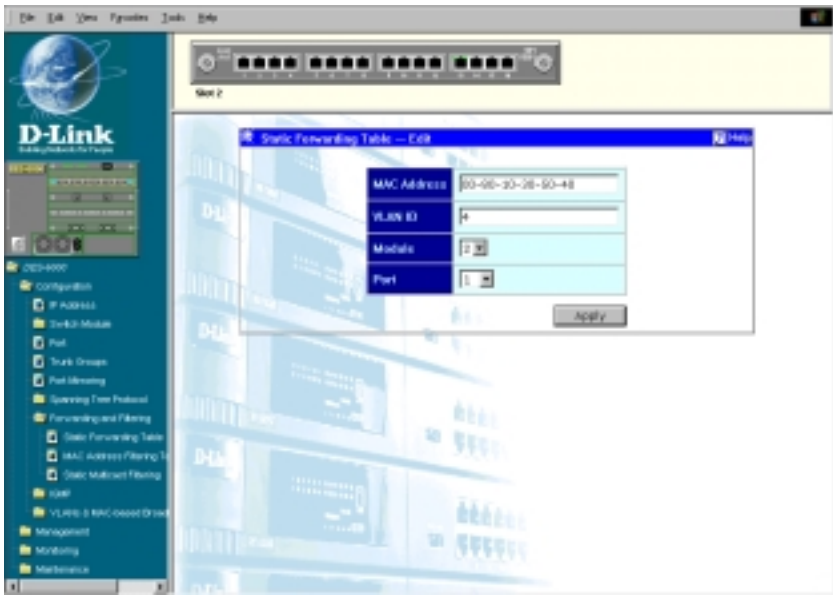


Figure 7-12. Static Forwarding Table --- Edit window

To use the MAC forwarding function, enter the MAC Address of the device to which the specified port permanently forwards traffic in the MAC address field. Then enter the VLAN ID, Module, and Port number that permanently forwards traffic from the specified device in the last three fields. Click **Apply** to let your changes take effect.

MAC Address Filtering Table

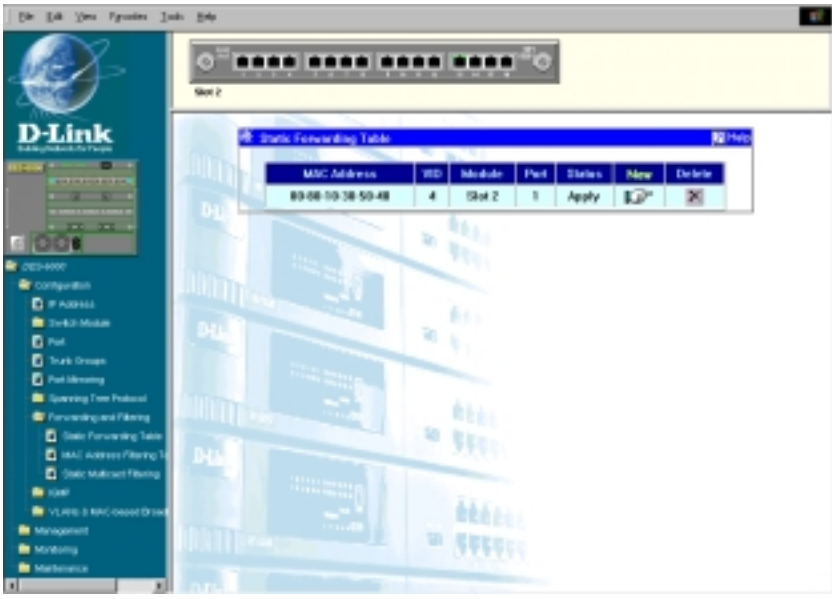


Figure 7-13. Static MAC Address Filtering window

The static filtering function filters out all traffic from unwanted devices by defining the MAC address to be filtered. All packets with the MAC address in the source or destination fields will be filtered. If VLANs are enabled, you must also specify the VID on which to filter the packets.

Click **New** to access the **Static MAC Address Filtering --- Edit** window:

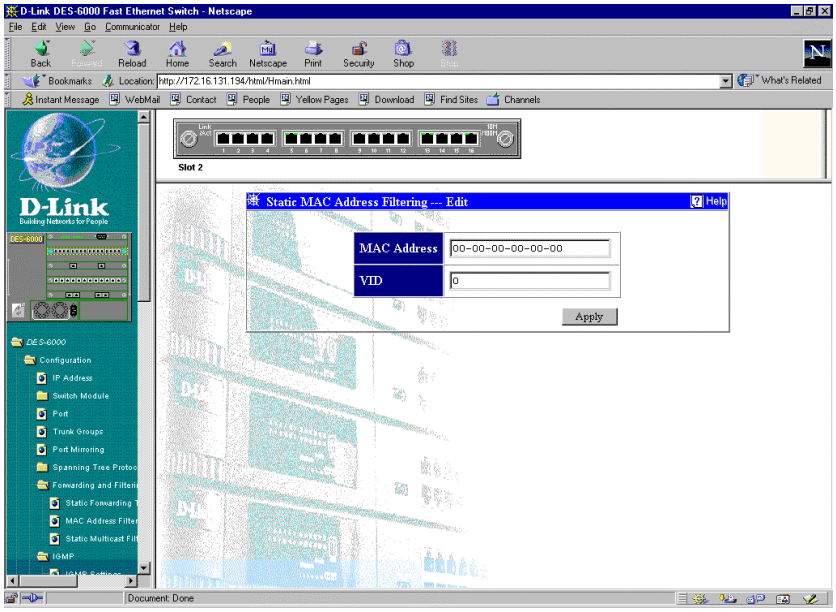


Figure 7-14. Static MAC Address Filtering --- Edit window

To add or modify a Static MAC Filtering table entry, enter the desired MAC address and VLAN ID in the two fields offered. Click **Apply** to let your changes take effect.

Static Multicast Filtering

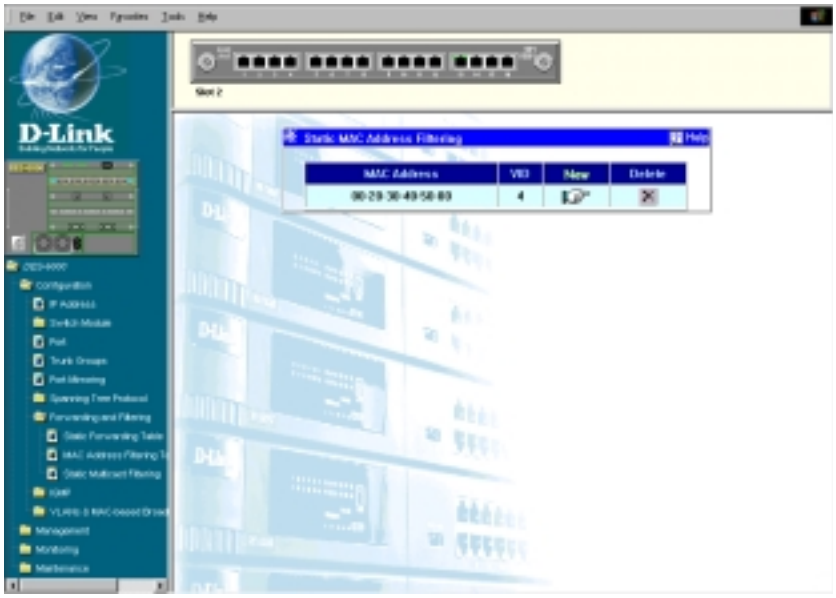


Figure 7-15. Static Permanent Multicast Filtering window

Static multicast filtering blocks or forwards traffic over each port for one multicast group. You can configure each port on the Switch to forward traffic for the specified multicast group. If VLANs are enabled, you must also specify the VID on which to filter the packets.

Click **New** to access the **Static Multicast Filtering --- Edit** window:

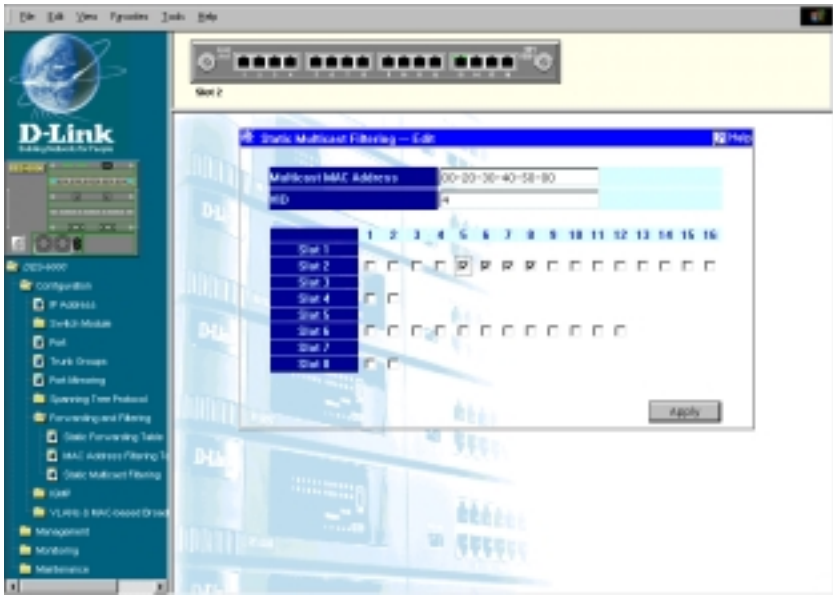


Figure 7-16. Static Multicast Filtering --- Edit window

To edit or create a new filter, enter the multicast MAC address in the Multicast MAC Address field, and select the desired VID (if VLANs are enabled) and ports which will receive the multicast packets. Click **Apply** to activate the filter. You must enter a valid multicast MAC Address. If you fail to do so and click the **Apply** button, you will return to the multicast filtering table, but your entry will not appear there. The VID option will only appear on screen if 802.1Q or Port-based VLANs are enabled.

IGMP

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP router. IGMP is used for managing IP multicast groups. The Switch will send IGMP query messages and get the IGMP response from hosts to "learn" the source port members of that multicast address. When a multicast address is received and found on the IGMP address table, it will be multicast to those port members.

IGMP Settings

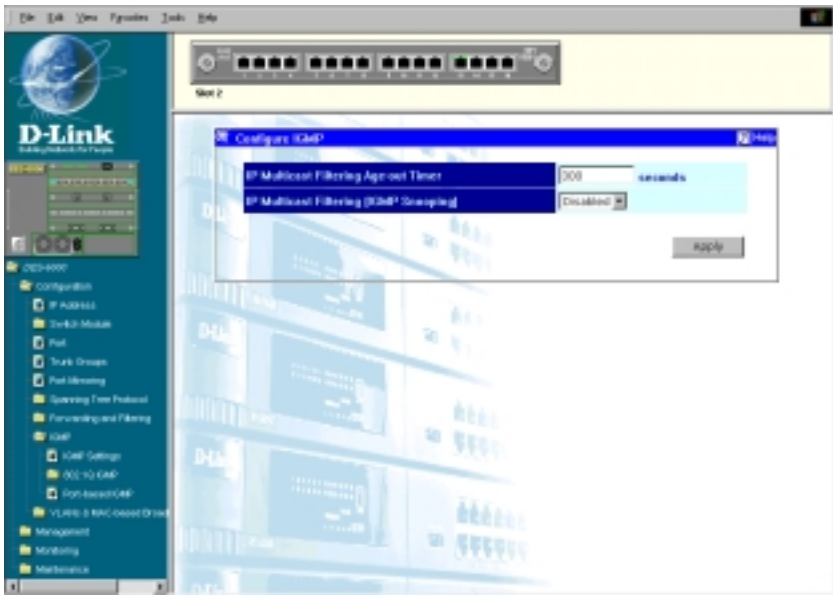


Figure 7-17. Configure IGMP window

To configure the IGMP, enter a value between 30 and 9999 seconds in the IP Multicast Filtering Age-out Timer field and then change the IP Multicast Filtering (IGMP Snooping) setting from *Disabled* to *Enabled*. Click the **Apply** button to let the changes take effect.

802.1Q IGMP

802.1Q IGMP allows you to adjust IGMP settings when 802.1Q VLANs are active on your network.

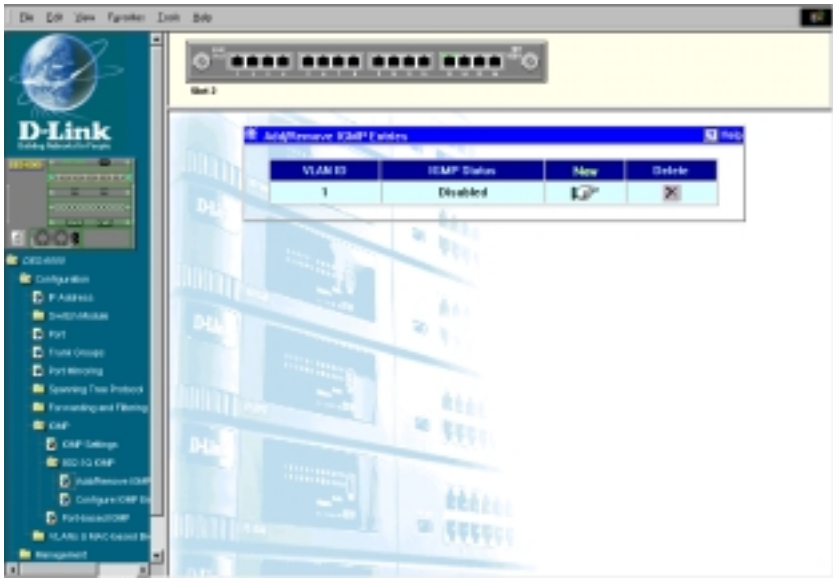


Figure 7-18. Add/Remove IGMP Entries window

Click the **X** in the Delete column next to an entry to remove it from the table.

Click the pointer icon or the **New** heading to access the **Add/Remove IGMP Entries --- Edit** window:

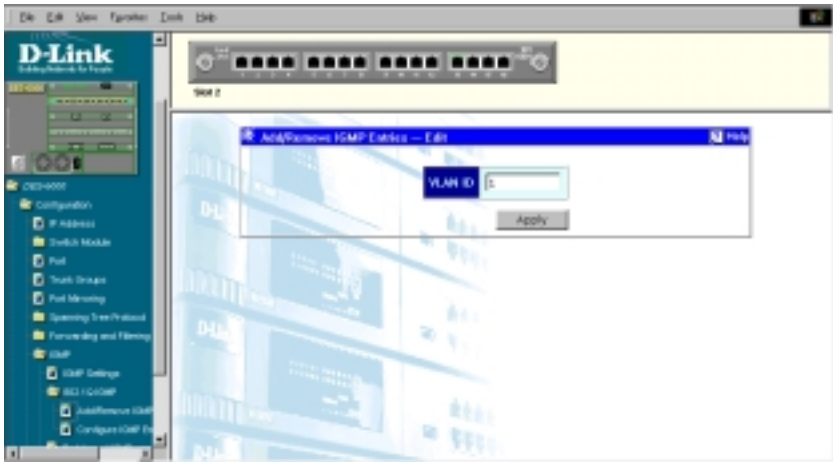


Figure 7-19. Add/Remove IGMP Entries --- Edit window

To edit an 802.1Q IGMP entry, enter a value from 1 to 4094 in the VLAN ID field and then click **Apply**.

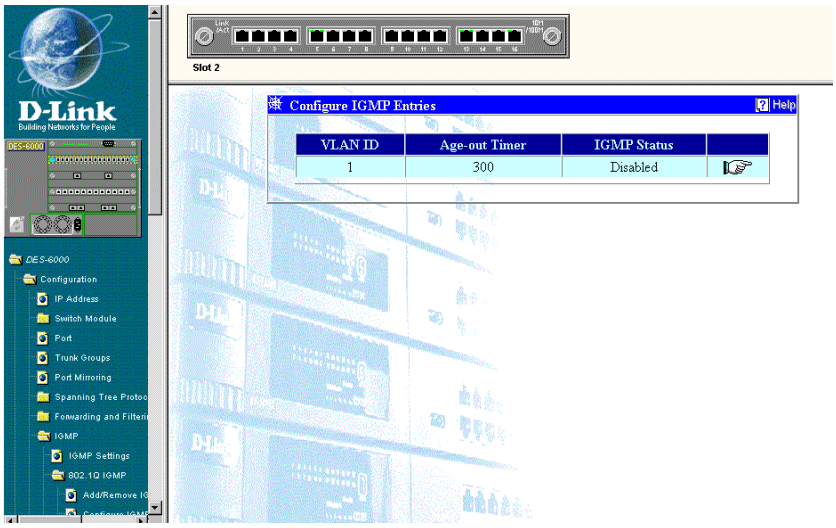


Figure 7-20. Configure IGMP Entries window

This window displays the VLAN ID, Age-out Timer setting, and IGMP status for IGMP entries.

To edit an IGMP entry, click the pointer icon on the window above. The **Configure IGMP Entries --- Edit** window appears:

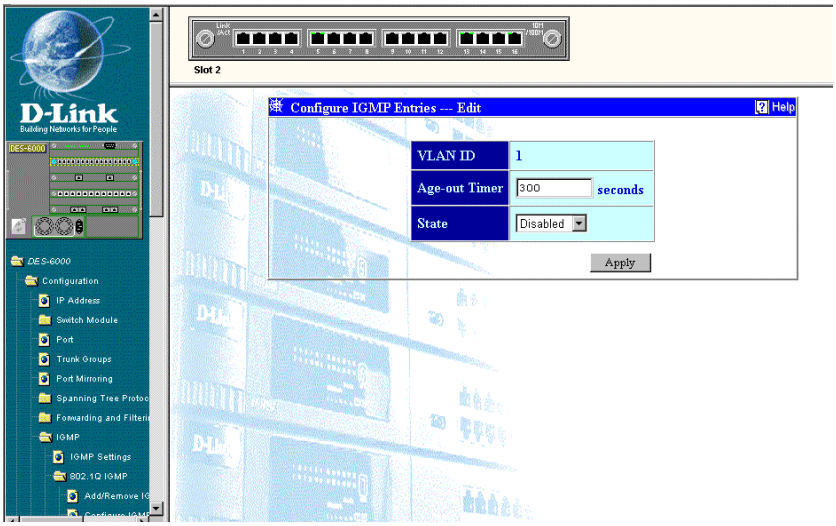


Figure 7-21. Configure IGMP Entries --- Edit window

To edit an IGMP entry, enter a value in the Age-out Timer field and then select *Enabled* or *Disabled* in the State field. Click **Apply** to let your changes take effect.

Port-based IGMP

Port-based IGMP allows you to adjust IGMP settings when port-based VLANs are active.

Figure 7-22. Port-based IGMP window

In this window, you can enable or disable IGMP Status for each port-based VLAN as well as set an Age-out Time. Click **Apply** to let your changes take effect.

VLANs & MAC-based Broadcast Domains

IEEE 802.1Q VLANs allow you to construct a port group as well as to reduce traffic. All packets are limited to members of the VLAN. MAC-based Broadcast Domains limit broadcast, multicast and unknown packets to members of the broadcast domain(s) defined here. For more information on this section, please refer to "*Switch Management Concepts*" chapter.

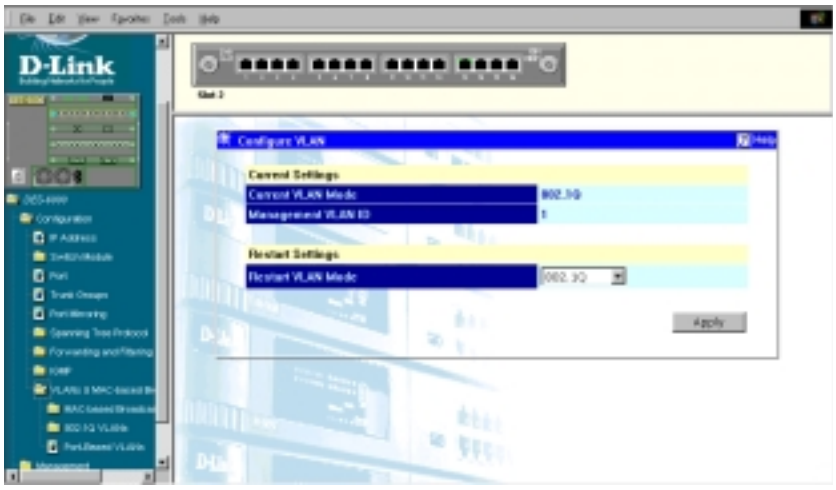


Figure 7-23. Configure VLAN window

To use the VLAN mode, select *MAC based* (broadcast domain), *802.1Q* or *Port based* under Restart VLAN Mode--otherwise, leave the setting at *Disabled*.

- **Restart VLAN Mode** Choose from four settings for this mode: *Disabled*, *MAC based* (broadcast domain), *Port based* or *802.1Q*. After being restarted, the Switch will implement the type of VLAN or broadcast domain chosen here.

- **Management VLAN ID** When *IEEE 802.1Q VLANs* are enabled, this is the VLAN that will be used for management packets. Make sure the switch port that the management station is connected to has this PVID number and is a member of this 802.1Q VLAN (VID). This should be the first VLAN you create, otherwise, you may not be able to communicate with the switch except through the console port. This setting can only be configured through the console connection. Web, Telnet, and MIB management stations can only view this setting as a read-only object.

After clicking the **Apply** button, go to the *Maintenance* section and choose **Save Changes**, and then restart the Switch to activate VLANs on the Switch.

MAC-Based Broadcast Domains

To use MAC-based broadcast domains, you must first create a MAC-based broadcast domain using the create/remove function and then add members to the broadcast domain using the Configure broadcast domain member function.

Figure 7-24. Create/Remove MAC-based Broadcast Domains window

- **Description** Lists all MAC-based broadcast domains.
- **Number of MAC address members** The number of MAC addresses belonging each MAC-based broadcast domain.

Click the X in the Delete column next to an entry to remove it from the table.

Click **New** to access the **Create/Remove MAC-based Broadcast Domains --- Edit** window:

Figure 7-25. Create/Remove MAC-based Broadcast Domains --- Edit window

To add a MAC-based broadcast domain, enter a description in the field offered. Click **Apply** to let the change take effect.

- **Description** The name of the MAC-based broadcast domain to be added to the switch.

After adding the VLAN, proceed to the Configure MAC-based Broadcast Domain Member screen to add members to the VLAN.

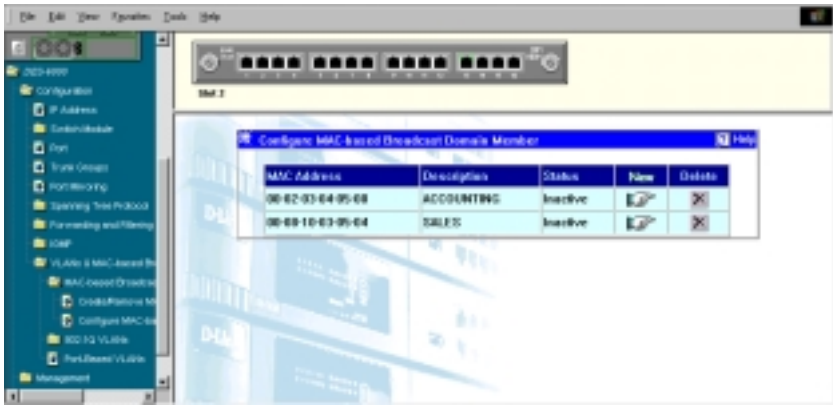


Figure 7-26. Configure MAC-based Broadcast Domain Member window

Items in this window are defined as follows:

- **MAC Address** The MAC Address of the broadcast domain member.
- **Description** The broadcast domain the member belongs to.
- **Status** Indicates whether the entry is *Active* or *Inactive*. To make entries active, the switch needs to be restarted in the appropriate VLAN or broadcast domain mode.

Click the **X** in the Delete column next to an entry to remove it from the table.

Click on the pointer icon to edit a specific entry, or click **New** to add an entry in the **Configure MAC-based Broadcast Domain Member --- Edit** window:

Figure 7-27. Configure MAC-Based Broadcast Domain Member --- Edit window

To add or edit a MAC-based broadcast domain member, enter the MAC address and description in the fields offered.

Items in this window are defined as follows:

- **MAC Address** The MAC address of the member you wish to add.
- **Description** The name of the broadcast domain to add a member to.

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

802.1Q VLANs

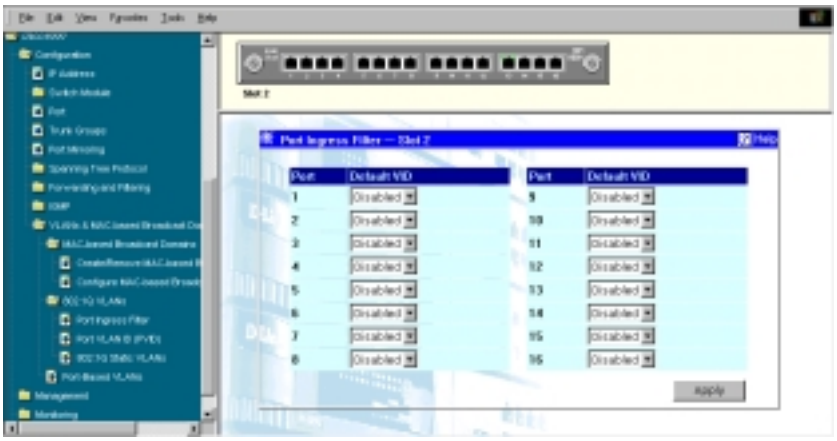


Figure 7-28. Port Ingress Filter window

Use this window to enable or disable the ingress filtering check for each desired port. Ingress filtering means that a receiving port will check to see if it is a member of the VLAN ID in the packet before forwarding the packet. Click **Apply** to let the settings take effect.

Figure 7-29. Port VLAN ID (PVID) window

Use this window to assign a Port VLAN ID (PVID) number for each port. Click **Apply** to let the settings take effect.

Figure 7-30. 802.1Q Static VLANs window

Click the **X** in the Delete column next to an entry to remove it from the table.

Click the pointer icon to access the **802.1Q Static VLANs --- Edit** window:

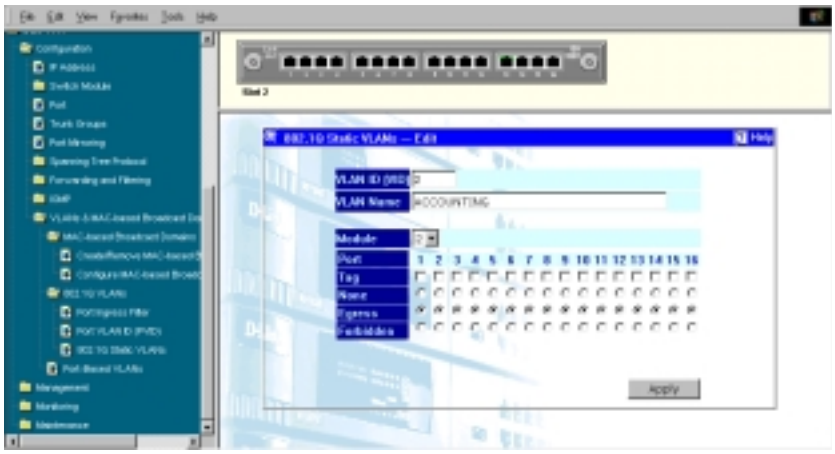


Figure 7-31. 802.1Q Static VLANs --- Edit window

To configure an 802.1Q VLAN entry, enter a VLAN ID (VID) number and VLAN Name in the first two fields. Next, select the desired Module. Finally, check Tag for each member port you wish to be a tagging port. None should be checked if you don't want a port to statically belong to a VLAN. Check Egress to statically set a port to belong to a VLAN. Check Forbidden if you wish to forbid the port from dynamically belonging to the VLAN. Click **Apply** to let the changes take effect.

Port-based VLANs

Port-based VLANs are a simplified version of 802.1Q VLANs. In port-based VLANs, each port can only belong to one VLAN, with all traffic remaining inside the VLAN.

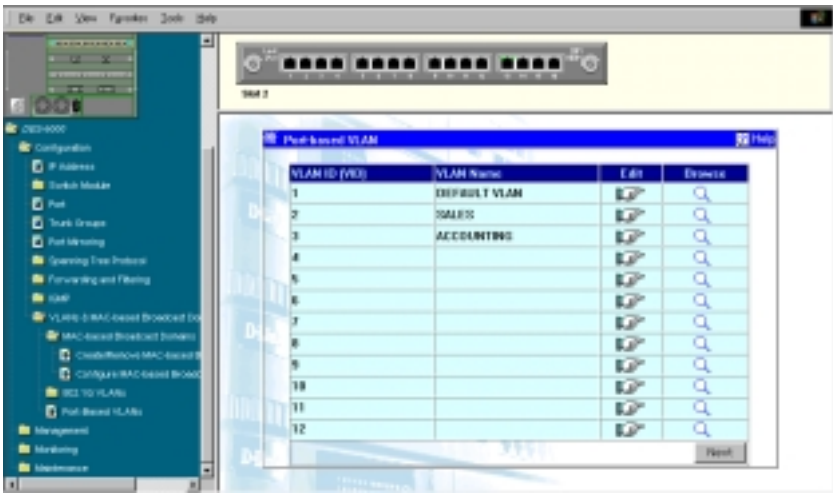


Figure 7-32. Port-based VLAN window

The above window lists all port-based VLANs currently setup on the Switch.

Click the pointer icon in the Edit column to access the **Port Based VLAN Entry** window:

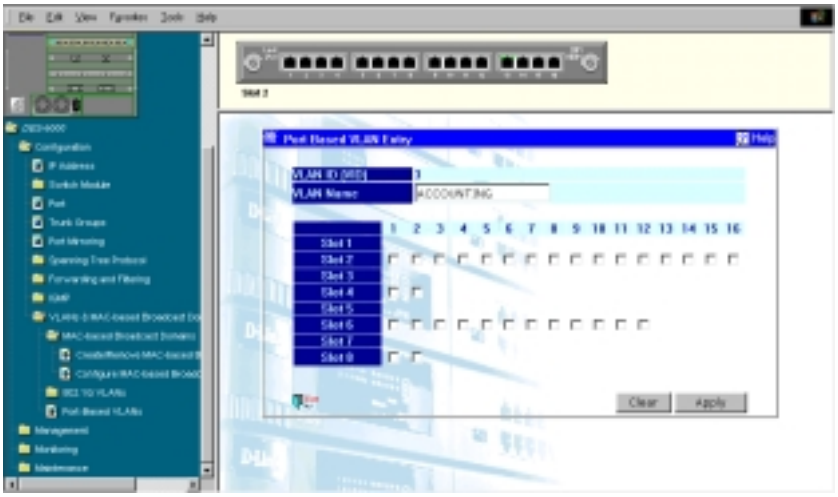


Figure 7-33. Port Based VLAN Entry window

The above window lists all ports in all modules currently installed in the Switch. To create a VLAN, type in a VLAN Name and then choose ports to belong to the VLAN. All computers connected to the chosen Switch ports will belong to the VLAN. If a port is grayed-out (inaccessible), it either belongs to another VLAN or is a non-anchor member of a Trunk group. Adding the anchor port to a VLAN automatically adds the other members of the trunk group.

Management

This second main category of the Switch Web-based management program includes: **Community Strings and Trap Receivers**, **User Accounts Management**, and **Console**.

Community Strings and Trap Receivers

Figure 7-34. Community Strings and Trap Receivers window

To use the functions on this window, enter the appropriate SNMP information in the Community Strings and Trap Receiving Station sections--you may enter up to four entries in each section. A trap receiving station is a device that constantly runs a network management application to receive and store traps. Then click **Apply** to put the settings into effect.

The SNMP Access Policy Setting section allows you to define SNMP communities on your network. This section is described as follows:

- **Community String** A user-defined SNMP community name.
- **Access Right** The permitted access of *Read-Only* or *Read-Write* using the SNMP community name.
- **Status** Option to activate or deactivate the current community string by setting it to *Valid* or *Invalid*.

The SNMP Trap Manager Configuration allows you to designate trap receivers. This section is described as follows:

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

User Accounts Management

User accounts are accounts set up on the Switch which allow access to the switch management features.

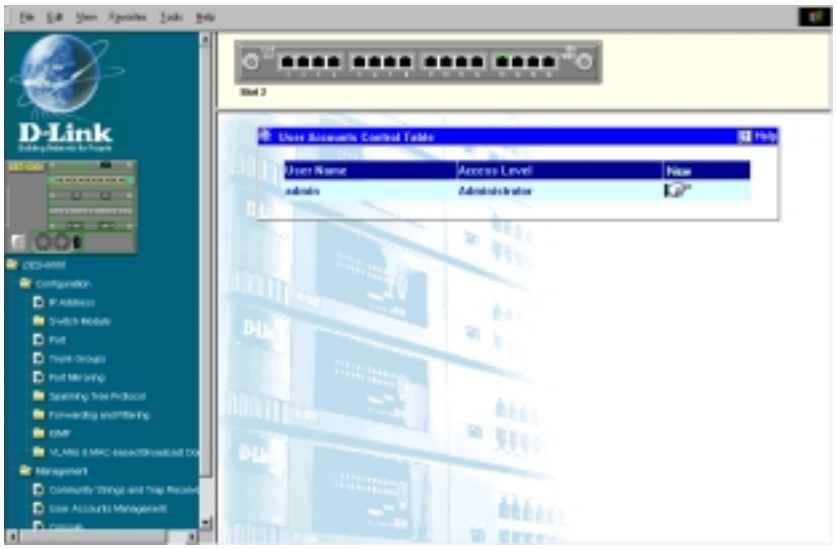


Figure 7-35. User Accounts Control Table window

Click the pointer icon in the New column to edit an account, or click on the New heading itself to add an account in the **User Accounts Control Table - Edit** window:

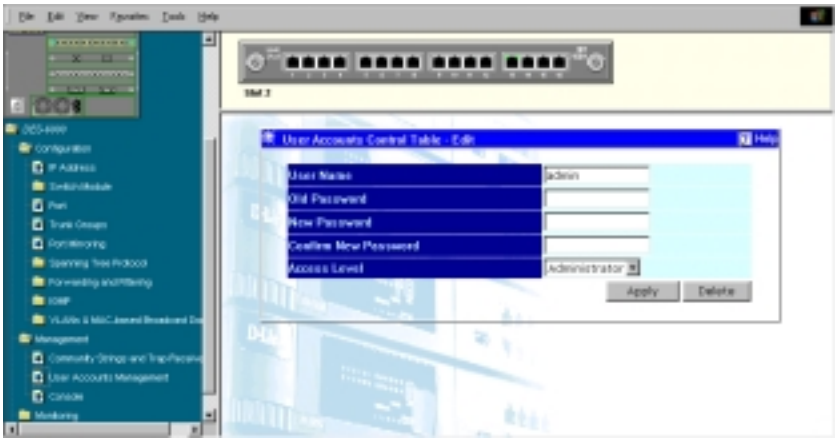


Figure 7-36. User Accounts Control Table - Edit window

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

To delete a User Account, enter the requested information and click **Delete**.

Console

The Console section allows you to configure settings for the console connection.

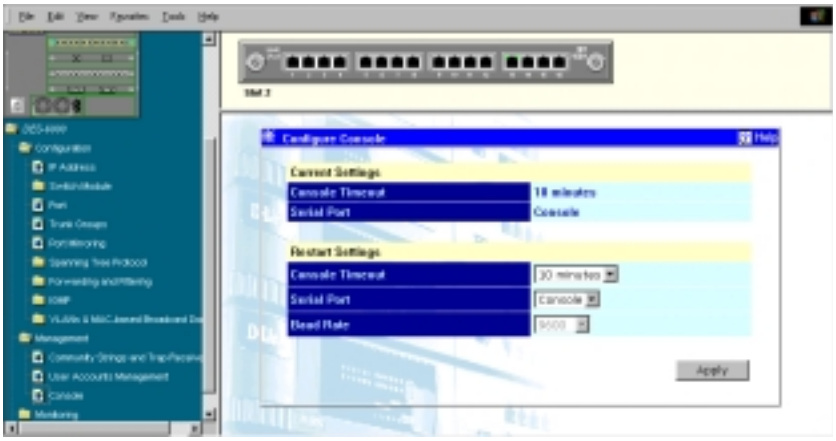


Figure 7-37. Configure Console window

Items in the window are described as follows:

- **Console Timeout** This is a security feature which measures the time that the console connection is inactive. Possible values are *2 mins*, *5 mins*, *10 mins*, *15 mins*, or *Never*. After the time expires the console will automatically log off.
- **Serial Port** Select the protocol for communicating through the console port, *Console* or *SLIP*. Use *SLIP* for out-of-band management.
- **Baud Rate** If *SLIP* is being used, you may set the Baud Rate to: *2400*, *9600*, *19200*, or *38400*.

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=X on/X off
- Parity=None
- Stop Bits=1

Monitoring

This third main category of the Switch Web-based management program includes: **Switch Overview**, **Port Utilization**, **Port Traffic Statistics**, **Port Error Packet Statistics**, **Port Packet Analysis**, **Browse Address Table**, **IP Multicast & IGMP Information**, **Switch History**, and **Device Status**.

Switch Overview

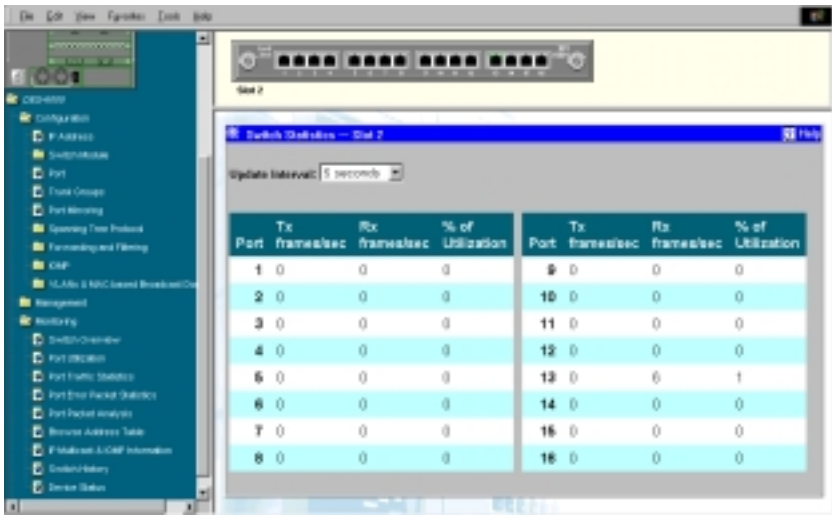


Figure 7-38. Switch Statistics window

The information is described as follows:

- **Update Interval** Choose the desired setting: *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*. The switch will be sampled for 1 second each update interval.
- **TX frames/sec** Counts the total number of frames transmitted to the segment connected to the ports during the single second just before the update interval.
- **RX frames/sec** Counts the total number of frames received from the segment connected to the ports during the single second just before the update interval.
- **% of Utilization** This shows the percentage of available bandwidth each port is using during the single second just before the update interval. For example, when a 10 Mbps port is relaying packets at 5 Mbps, the utilization is 50%.

Port Utilization

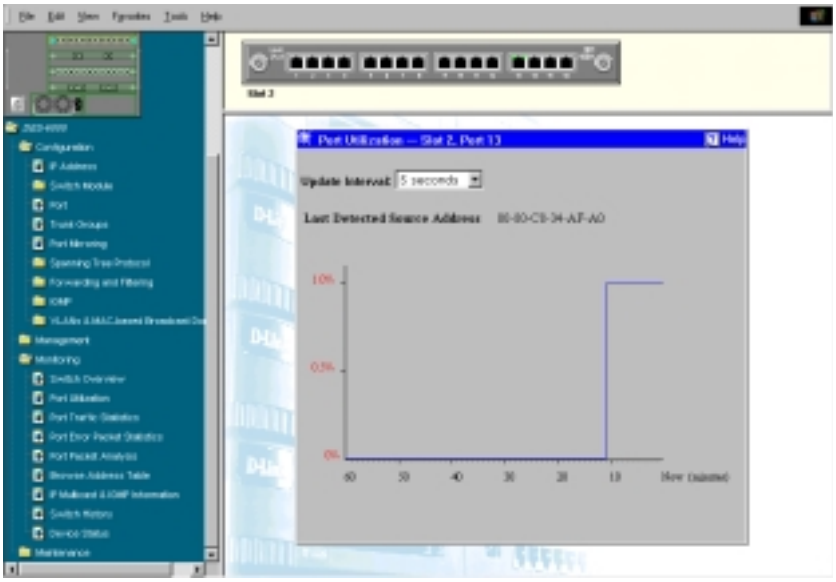


Figure 7-39. Port Utilization window

The information is described as follows:

- **Update Interval** Choose the desired setting: *5 seconds, 15 seconds, 30 seconds, 60 seconds* or *Suspend*.
- **Last Detected Source Address** The MAC address of the last device that sent packets over this port.

Port Traffic Statistics

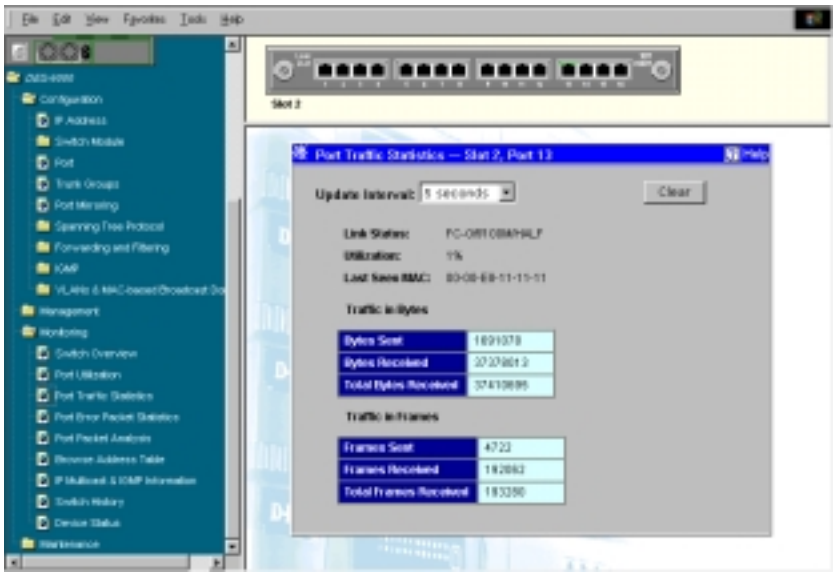


Figure 7-40. Port Traffic Statistics window

The port statistics shown by default are those for the port you last configured. Once in the individual window, you can click any port on the Switch graphic at the top of the window to show statistics for that port.

The information is described as follows:

- **Update Interval** Choose the desired setting: *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.
- **Clear button** Clicking on this button resets all counters in the tables on this page to the value zero.
- **Link Status** Indicates whether the port is online and working, in which case it displays the type of link, or whether the link is offline or not working.
- **Utilization** Current utilization for the port, as a percentage of total available bandwidth.
- **Last Seen MAC** The MAC address of the last device that sent packets over this port.

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.

Port Error Packet Statistics

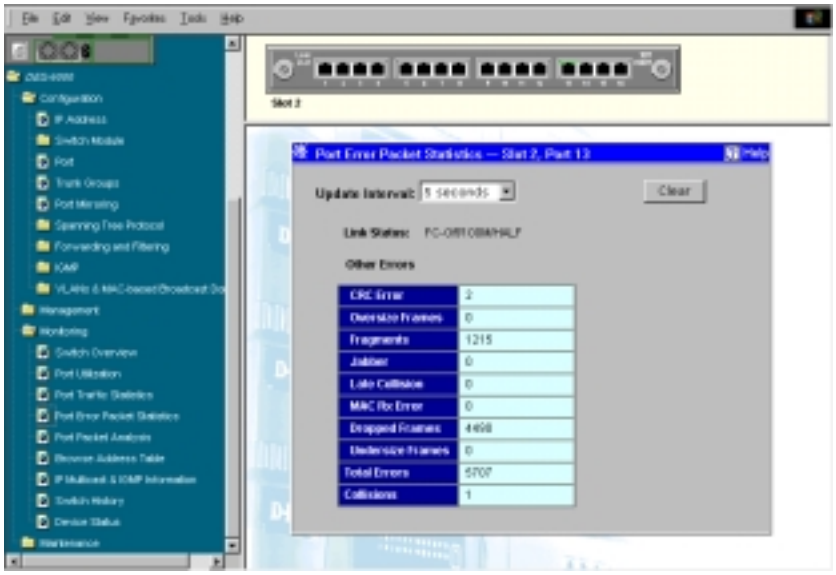


Figure 7-41. Port Error Packet Statistics window

The information is described as follows:

- **Update Interval** Choose the desired setting: *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.

- **Clear button** Clicking on this button resets all counters in the tables on this page to the value zero.
- **Link Status** Indicates the current link status.

Other errors:

- **CRC Error** Counts otherwise valid frames that did not end on a byte (octet) boundary.
- **Oversize Frames** Counts packets received that were longer than 1536 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Fragments** The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
- **Jabber** The number of frames with length more than 1536 bytes and with CRC error or misalignment (bad framing).
- **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 Rx Error** Counts data errors detectable as 100BASE-TX "symbol errors," bit patterns with illegal encodings. This may indicate noise on the line.
- **Dropped Frames** The number of frames which are dropped by this port since the last Switch reboot.
- **Undersize Frames** The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
- **Total Errors** The sum of the CRC Error, Oversize Frames, Fragments, Jabber, Late Collision, MAC Rx Error, Dropped Frames, and Undersize Frames counters.
- **Collisions** The total number of collisions on this Ethernet segment.

Port Packet Analysis

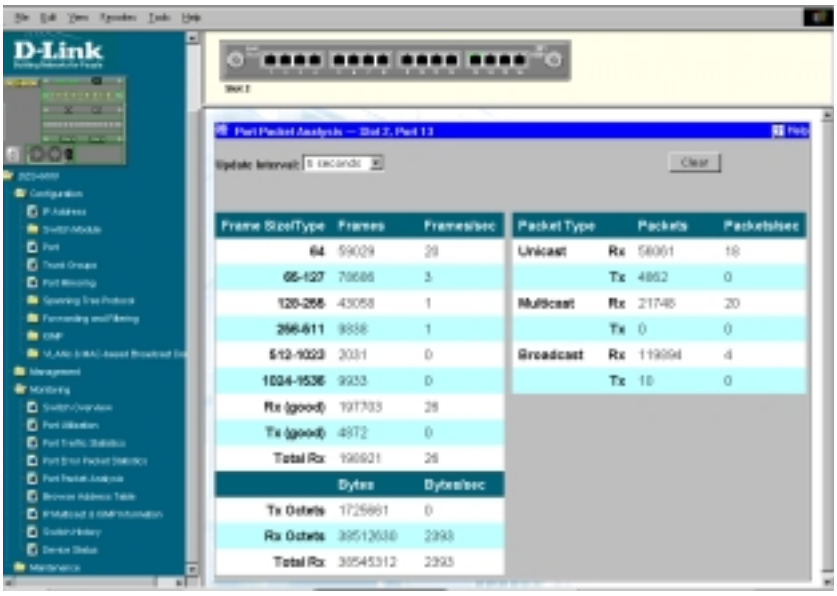


Figure 7-42. Port Packet Analysis window

The information is described as follows:

- **Update Interval** Choose the desired setting: *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.
- **Clear button** Clicking on this button resets all counters in the tables on this page to the value zero.
- **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).
- **1024-1536** The total number of packets (including bad packets) received that were between 1024 and 1536 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 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/Tx** The total number of good packets that were received by and directed to a unicast address. Note that this does not include dropped unicast packets
- **Multicast Rx/Tx** The total number of good packets that were received by and directed to a multicast address. Note that this number does not include packets directed to the broadcast address
- **Broadcast Rx/Tx** The total number of good packets that were received by and directed to a broadcast address. Note that this does not include multicast packets.

Browse Address Table

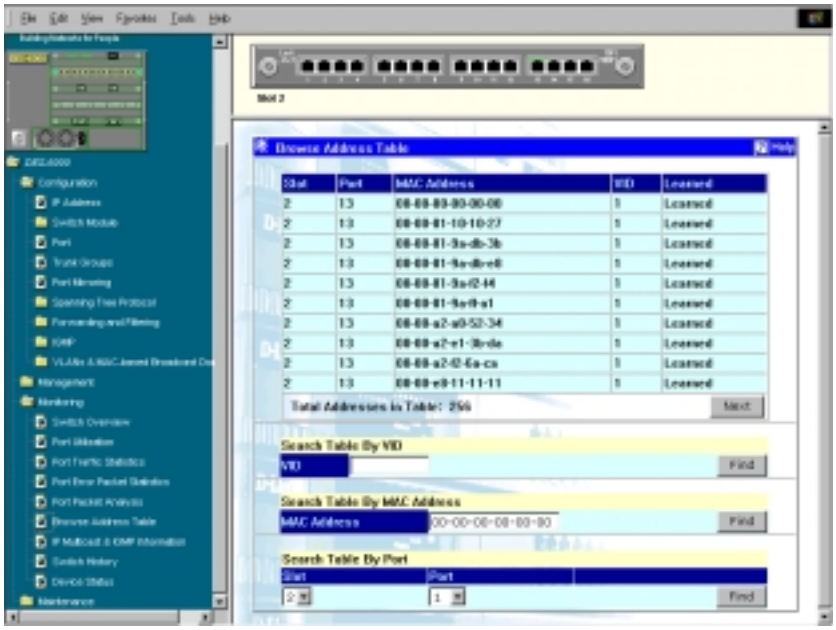


Figure 7-43. Browse Address Table window

The Switch allows you to display a table containing Switch ports, MAC addresses, and respective learned statuses. If the table doesn't display the information you want, fill in the requested information in the Search Table by VID, Search Table by MAC Address or Search Table by Port sections above and then click the **Find** button on the right side of the section used. Please note that the VID field will only be shown when VLANs are enabled on the Switch.

IP Multicast & IGMP Information

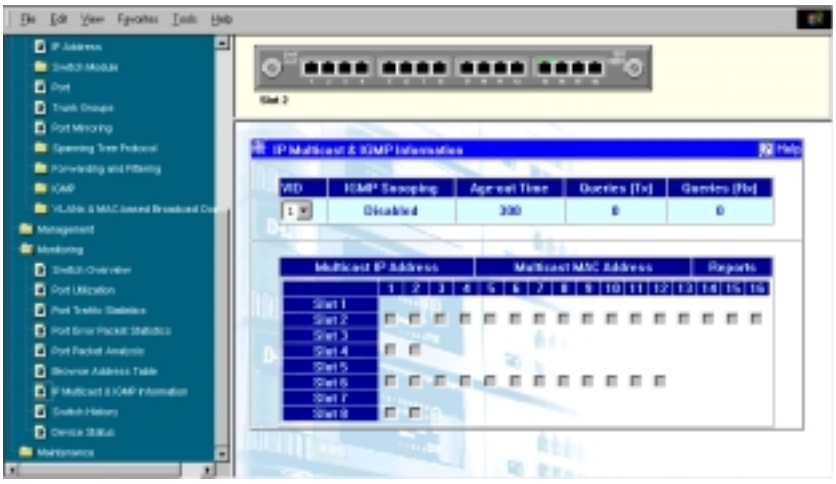


Figure 7-44. IP Multicast & IGMP Information window

This window allows you to enter a VID at the top of the window and then display the Queries (Tx)/(Rx) for that VLAN ID. The bottom of the window displays Multicast IP Address, Multicast MAC Address, Reports, and Ports in a table format. Enabling IGMP Snooping allows you to view IP Multicast and IGMP Information across your entire network.

Switch History

This screen allows you to view the switch logs.

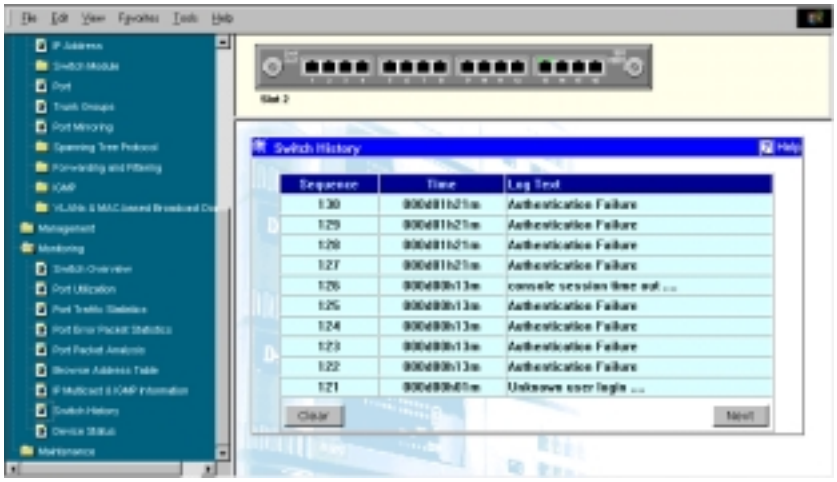


Figure 7-45. Switch History window

This window allows you to view the Switch history. This works like a trap and event receiver except it only captures trap/events generated by the Switch itself. Click the **Next** button to view additional pages. Clicking on the **Clear** button empties the switch history.

Device Status

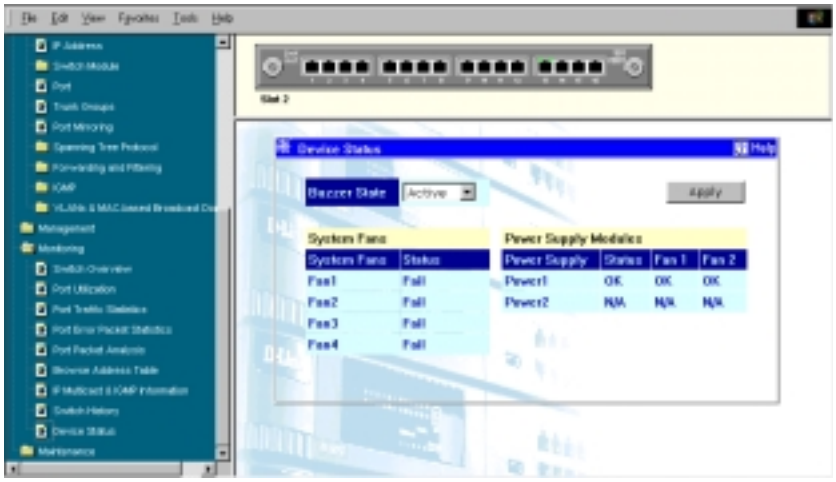


Figure 7-46. Device Status window

This screen allows you to activate/deacivate the switch alarm in the Buzzer State field, which will sound when one of the system fans or power supplies fails. It also displays the current status of the System Fans and Power Supply Modules.

Maintenance

The fourth and last main category of the Switch Web-based management program includes: **Firmware and Configuration Update**, **Save Settings To TFTP Server**, **Save Switch History To TFTP Server**, **Clear Address Table**, **Save Changes**, **Factory Reset**, and **Restart System**.

Firmware and Configuration Update

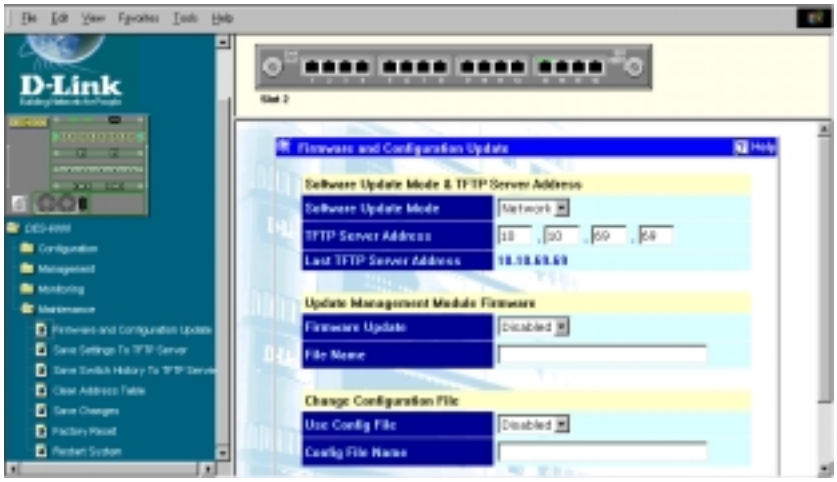


Figure 7-47. Firmware and Configuration Update window

To update the switching software (firmware) or load settings from a configuration file, fill in the requested information above and then click the **Apply** button.

The information is described as follows:

Software Update Mode & TFTP Server Address:

- **Software Update Mode** Set to either *Network* or *SLIP*. Determines whether the new firmware code or 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 new firmware image file or configuration file is located.
- **Last TFTP Server Address** This read-only field displays the IP address of the last TFTP server used.

Update Management Module Firmware:

- **Firmware Update** Determines whether or not the Switch should download its new firmware code the next time it is restarted.
- **File Name** The path and the name on the TFTP server which holds the new firmware image file.

Change Configuration File:

- **Use Config File** Toggle to *Enabled* to use a configuration text file when the Switch is reset (rebooted). Determines whether or not the Switch should retrieve settings from a configuration file the next time it is booted.
- **Config File Name** The complete path and filename on the TFTP server for the configuration file to use. The configuration file is a text file containing IP settings for the switch. Please refer to the "*Sample Configuration File*" appendix at the back of this manual for more information on creating a configuration file.

Save Settings to TFTP Server

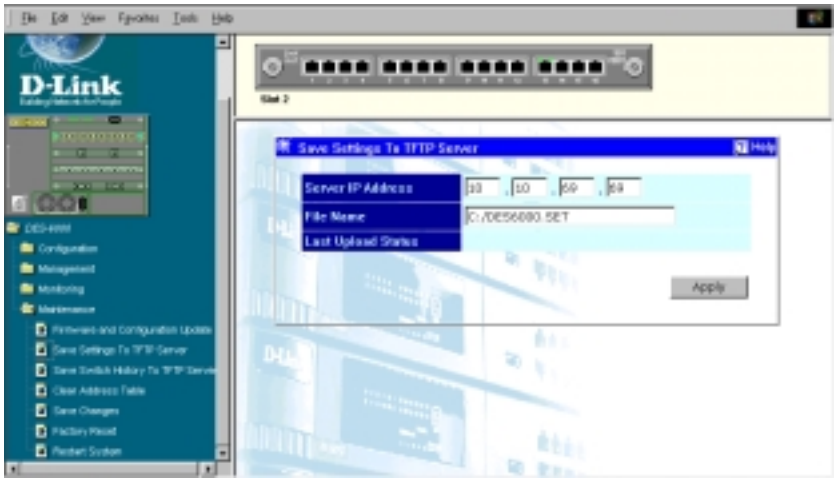


Figure 7-48. Save Settings to TFTP Server window

To save your current settings to a configuration file, enter the TFTP Server IP Address where the configuration file is to be located and the complete path and File Name. Then click the **Apply** button.

Please note that the settings will be saved from the NV-RAM. Make sure you have **Saved Changes** before saving the settings.

The information is described as follows:

- **Server IP Address** The IP address of the TFTP server where the configuration file is.
- **File Name** The path and file name for the configuration file on the TFTP server.
- **Last Upload Status** Shows whether the attempt to upload software was successful or not by displaying either "Success" or "Fail."

Save Switch History to TFTP Server

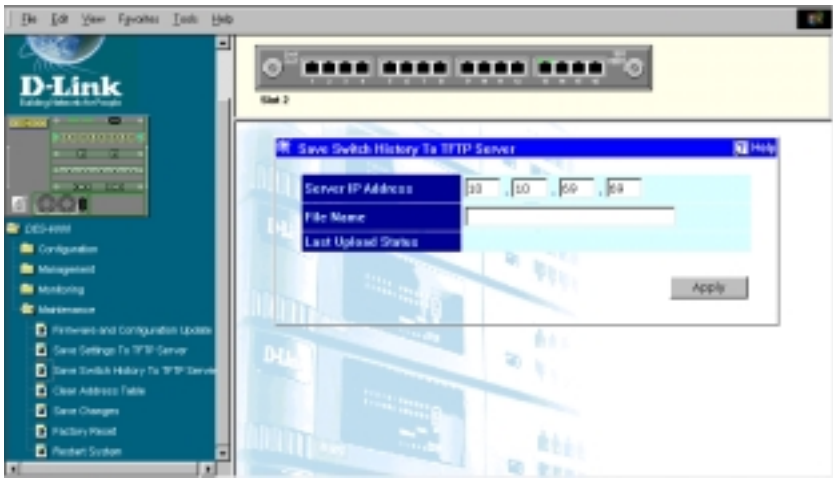


Figure 7-49. Save Switch History to TFTP Server window

To save the switch logs to your TFTP server, fill in the fields above and then click **Apply**.

The information is described as follows:

- **Server IP Address** The IP address of the TFTP server where the log file will be saved.
- **File Name** The path and file name for the file to be saved on the TFTP server.
- **Last Upload Status** Shows whether the attempt to upload software was successful or not by displaying either "Success" or "Fail."

Clear Address Table

Figure 7-50. Clear Address Table window

Click on the **Apply** button to clear the Switch's forwarding table.

Save Changes

Figure 7-51. Save Changes window

To save all the changes made in the current session to the Switch's flash memory, click the **Save Configuration** button. Once in the NV-RAM, they become the default settings for the Switch and are impervious to System Restarts or power downs.

Factory Reset

Figure 7-52. Factory Reset to Default Value window

Doing a factory reset will return all settings to their original values at the time of purchase. After performing a factory reset, the Switch will need to be entirely reconfigured from scratch. Click the **Reset to Factory Default** button to initiate the reset.

Restart System

Figure 7-53. Restart System window

To reboot the Switch, which resets the system to values stored in NV-RAM, click the **Restart** button. If you have made changes to the settings during this session and wish to keep the changes, make sure **Yes** box is checked.

A

TECHNICAL SPECIFICATIONS

General		
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX/LX Gigabit Ethernet IEEE 802.1p/q IEEE 802.3x	
Protocol	CSMA/CD	
Data Transfer Rate Ethernet Fast Ethernet: Gigabit Ethernet:	**Half-duplex** 10 Mbps 100 Mbps n/a	**Full-Duplex** 20 Mbps 200 Mbps 2000 Mbps
Topology	Star	
Network Cables 10BASE-T: 100BASE-TX:	 2-pair Category 3/4/5 UTP (max. 100 m) EIA/TIA-568 100-ohm STP (max. 100 m) 2-pair Category 5 UTP (max. 100 m) EIA/TIA-568 100-ohm STP (max. 100 m)	

Physical and Environmental	
AC Input	90 to 264 VAC, 47-63 Hz (auto-adjusting internal power supply)
DC Fans	Two built-in 60 x 60 mm fans per power supply unit
Temperature	Operating: 0° to 40° C (32° to 104° F) Storage: -25° to 55° C (-13° to 131° F)
Relative Humidity	Operating: 5% to 95% (non-condensing) Storage: 0% to 95% (non-condensing)
Dimensions	H: 35.6 cm (14.01 in.) W: 44.0 cm (17.32 in.) D: 29.4 cm (11.57 in.)
EMI	FCC Class A, CE Class A, VCCI Class A, BSMI Class A, C-Tick Class A
Safety	UL/CUL, TUV, CE

B

RJ-45 PIN SPECIFICATION

When connecting the Switch to another switch, a bridge or a hub, a modified crossover cable is necessary. Please review these products for matching cable pin assignment.

The following diagram and table show the standard RJ-45 receptacle/connector and their pin assignments for the switch-to-network adapter card connection, and the straight/crossover cable for the Switch-to-switch/hub/bridge connection.

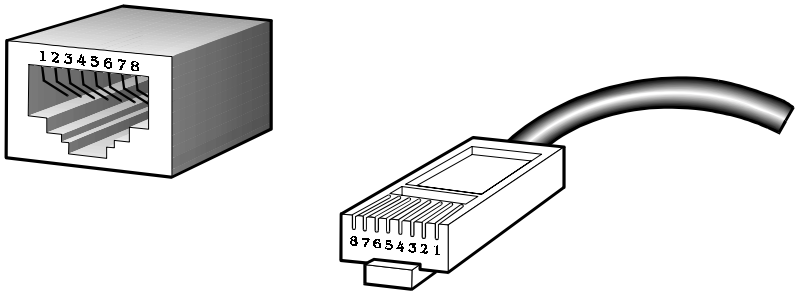


Figure B-1. The standard RJ-45 receptacle/connector

RJ-45 Connector pin assignment	
Contact	Media Direct Interface Signal
1	Tx + (transmit)
2	Tx - (transmit)
3	Rx + (receive)
4	Not used
5	Not used
6	Rx - (receive)
7	Not used
8	Not used

Table B-1. The standard Category 3 cable, RJ-45 pin assignment

The following shows straight cable and crossover cable connection:

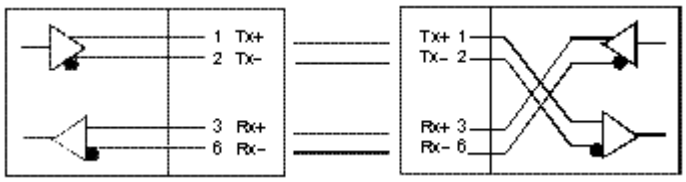


Figure B-2. Straight cable for Switch (uplink MDI-II port) to switch/Hub or other devices connection

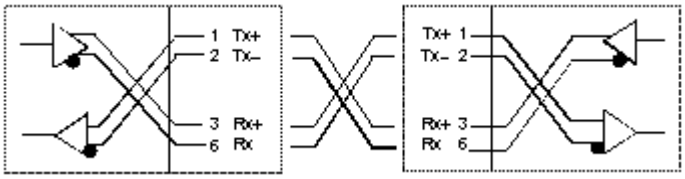


Figure B-3. Crossover cable for Switch (MDI-X port) to switch/hub or other network devices (MDI-X port) connection

C

SAMPLE CONFIGURATION FILE

This appendix provides a sample configuration file that can be used with the **Update Firmware and Configuration Files** screen in the console program.

The configuration file is a simple text file that you create. It has two functions: to point to the location of a file on a TFTP server, and to set the IP address, subnet mask and default gateway for the Switch. The file being uploaded can be either new runtime switching software, or a switch settings file which was previously saved on the TFTP server using the **Save Settings to TFTP Server** screen on the **System Utilities** menu. The IP address settings defined in the configuration file will override all other IP settings, even those defined in the settings file being uploaded. This enables the settings from one switch to be uploaded to another switch without their IP settings being the same (and thus coming into conflict).

Commands:

- `Code_type` – This command tells the Switch the type of file you wish to upload to the Switch. Possible Code_types are `PROM`, `RUNTIME`, or `CONFIG`. This should always be the first setting.
  - PROM – PROM update file.
  - RUNTIME – Switching software update file.
  - CONFIG – Image file of switch settings created by the settings backup procedure.
- `Image_file` – This command tells the switch the complete path and filename for the file to be loaded into the switch. For example, "`e:\6000\6000prom.tfp`". Make sure double-quotes are used as in the example file below.
- `Ip_addr` – This is the IP address that will be assigned to the switch. This command is included for downloading a configuration settings file to another switch. The IP address defined in this file will override the IP address in the configuration settings file, thus the switch you are downloading to can have a different IP address than the one that created the configuration settings file. An example of an IP address is: `10.12.19.102`.
- `Subnet_mask` – This is the subnet mask that will be assigned to the switch. An example of a subnet mask is: `255.128.0.0`.
- `Default_gateway` – This is the default gateway IP that will be assigned to the switch. An example of a default Gateway IP is: `10.254.254.253`.
- # – Remark. When placed as the first character on a line, the entire line will be ignored by the switch. This allows items to be labeled, or unused commands to remain in the file so that the syntax will not be forgotten.

Notes about the Configuration File:

This configuration file can only contain 4 settings: `Code_type`, `Ip_addr`, `Subnet_mask` and `Default_gateway`.

Each command can only appear once in the configuration file.

If both the Firmware Update and Use Config File options are enabled, the Firmware Update command will take precedence and only the firmware file will be uploaded to the switch.

The Config image file, which contains all configuration settings and was created by the switch is prefixed with the version number of the runtime software to help with file management.

```
# Sample Config File

Code_type=PROM
Image_file="e:\6000\6000prom.tfp"

# specify IP address
Ip_addr = 10.12.19.102

# specify subnet mask
Subnet_mask = 255.128.0.0

# specify default gateway
Default_gateway = 10.254.254.253
```

D

RUNTIME SOFTWARE DEFAULT SETTINGS

Load Mode	Network Ethernet
Configuration update	Disable
Firmware update	Disable
Out-of-band baud rate	9600
Rs232 mode	Console
Ip address	0.0.0.0
Subnet mask	0.0.0.0
Default router	0.0.0.0
Bootp service	Enable
TFTP server IP address	0.0.0.0
IGMP time out	300 secs
IGMP snooping state	Disable
Partition mode	Enable
Address table lock	Disable
Device HOL	Enable
Port HOL	Enable
Console time out	15 min
User name	[none]
Password	[none]
Device STP	Disable
Port STP	Enable
Port enable	Enable
Bridge max age	20 secs
Bridge hello time	2 sec
Bridge forward delay	15 sec
Bridge priority	32768
Port STP cost	100 (10M), 19 (100M), 4 (1000M)
Port STP priority	128
Forwarding MAC address aging time	300 secs
Address lookup mode	Level 1
NWay	Enable`
Flow control	Enable
Backpressure	Disable
Port lock	Disable
Port priority	Normal
Broadcast storm rising action	Do nothing
Broadcast storm falling action	Do nothing
Broadcast storm rising threshold	Default
Broadcast storm falling threshold	Default
Community string	"public", "private"
VLAN mode	Disable
SNMP VLAN(802.1Q)	1
Default port VID	1
Ingress rule checking	Disable
Mirror src port <->target port	1←2
Mirror	Disable

INDEX

D-Link® Offices

AUSTRALIA **D-LINK AUSTRALASIA**
Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077
TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand)
URL: www.dlink.com.au E-MAIL: support@dlink.com.au, info@dlink.com.au

CANADA **D-LINK CANADA**
2180 Winston Park Drive, Oakville, Ontario L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223 BBS: 1-965-279-8732
FREE CALL: 1-800-354-6522 URL: www.dlink.ca
FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca

CHILE **D-LINK SOUTH AMERICA**
Isidora Goyenechea #2934 of.702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-2320923 URL: www.dlink.cl
E-MAIL: ccasassu@dlink.cl, tsilva@dlink.cl

DENMARK **D-LINK DENMARK**
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL:45-43-969040 FAX:45-43-424347 URL: www.dlink.dk
E-MAIL: info@dlink.dk

EGYPT **D-LINK MIDDLE EAST**
7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-2456176 FAX: 202-2456192 URL: www.dlink-me.com
E-MAIL: support@dlink-me.com, fateen@dlink-me.com

FRANCE **D-LINK FRANCE**
Le Florilege #2, Allee de la Fresnerie
78330 Fontenay Le Fleury France
TEL: 33-1-30238688 FAX: 33-1-3023-8689
URL: www.dlink-france.fr E-MAIL: info@dlink-france.fr

GERMANY **D-LINK GERMANY**
Bachstrae 22, D-65830 Kriftel Germany
TEL: 49-(0)6192-97110 FAX: 49-(0)6192-9711-11
URL: www.dlink.de BBS: 49-(0)6192-971199 (Analog) 49-(0)6192-971198 (ISDN)
INFO LINE: 00800-7250-0000 (toll free) HELP LINE: 00800-7250-4000 (toll free)
REPAIR LINE: 00800-7250-8000 E-MAIL: mbischoff@dlink.de, mboerner@dlink.de

INDIA **D-LINK INDIA**
Plot No.5, Kurla-Bandra Complex Road,
Off Cst Road, Santacruz (E), Bombay - 400 098 India
TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: www.dlink-india.com
E-MAIL: service@dlink.india.com

ITALY **D-LINK ITALY**
Via Nino Bonnet No. 6/b, 20154 Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 E-MAIL: info@dlink.it URL: www.dlink.it

JAPAN **D-LINK JAPAN**
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141 Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp
E-MAIL: kida@d-link.co.jp

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

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

S. AFRICA **D-LINK SOUTH AFRICA**
Unit 2, Parkside 86 Oak Avenue
Highveld Technopark Centurion, Gauteng, Republic of South Africa
TEL: 27(0)126652165 FAX: 27(0)126652186 CELL NO: 0826010806 (Bertus Moller)
CELL NO: 0826060013 (Attie Pienaar) E-MAIL: bertus@d-link.co.za, attie@d-link.co.za

SWEDEN **D-LINK SWEDEN**
P.O. Box 15036, S-167 15 Bromma Sweden
TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901 E-MAIL: info@dlink.se
URL: www.dlink.se

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

U.K. **D-LINK EUROPE**
D-Link House, 6 Garland Road, Stanmore, London HA7 1DP U.K.
TEL: 44-20-8235-5555 FAX: 44-20-8235-5500 BBS: 44-20-8235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. **D-LINK U.S.A.**
53 Discovery Drive, Irvine, CA 92618 USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033 INFO LINE: 1-800-326-1688
BBS: 1-949-455-1779, 1-949-455-9616
URL: www.dlink.com E-MAIL: tech@dlink.com, support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____
Organization: _____Dept. _____
Your title at organization:_____
Telephone:_____ Fax:_____
Organization's full address: _____
_____
Country: _____
Date of purchase (Month/Day/Year): _____

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

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____
Telephone:_____ Fax:_____
Reseller's full address: _____
_____
_____

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

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

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

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

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

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

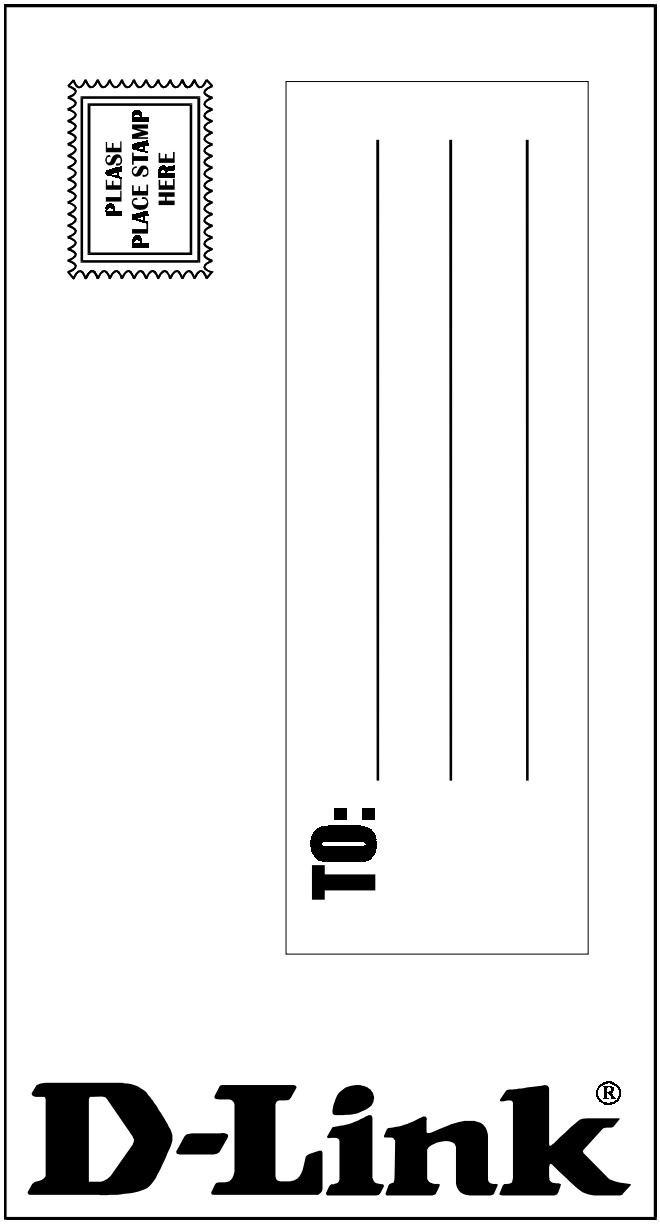
6. What network medium/media does your organization use ?
☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

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

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

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

10.Your comments on this product?
_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®