D-Link®

DES-3624 Series Stackable NWay Ethernet Switch User's Guide

First Edition (Dec., 1999)
6DES3624..01
Printed In Taiwan

RECYCLABLE

Wichtige Sicherheitshinweise

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

WARRANTIES EXCLUSIVE

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

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

LIMITATION OF LIABILITY

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

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

Limited Warranty

Hardware:

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

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

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

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

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

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

Software:

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

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

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

D-Link Offices for Registration and Warranty Service

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

Trademarks

Copyright Statement

FCC Warning

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

CE Mark Warning

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

VCCI Warning

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

BSMI Warning

警 告 使 用 者

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

TABLE OF CONTENTS

FIGURES AND TABLES

ABOUT THIS GUIDE

This User's Guide tells you how to install your Stackable NWay 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 (please note that Netscape Communicator/Navigator, 4.x or later, or Microsoft Internet Explorer, 4.x or later, are recommended).

Conventions

References in this manual to the DES-3624 Series are frequently written simply as "Switch" or "Switches" where the text applies to all models. Model numbers are normally used only to differentiate among specific Switches where necessary.

Unless differentiated by model number, all information applies to all 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, rear panel, 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.
- 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-3624 series of Switches can include one master (either a DES-3624i or a DES-3624iF) and up to three clients (DES-3624 or DES-3624F). They are 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:

Ports

- 20 high performance NWay ports all operating at 10/100 Mbps for connection to servers and hubs (19 ports 10/100 fixed Ethernet TP interface and one MDI-II/MDI-X jack connection are supported) (DES-3624i and DES-3624iF) or 22 high performance NWay ports all operating at 10/100 Mbps for connection to servers and hubs (20 ports 10/100 fixed Ethernet TP interface and two MDI-II/MDI-X jack connections are supported) (DES-3624 and DES-3624F).

- All ports can be auto-negotiated between 10Mbps/100Mbps, half-duplex or full duplex connections.
- Gigabit uplink/MDI-II (media dependent interface) slide-in module in the rear panel for uplink to another Switch. One-port or two-port models are available (DES-3624i and DES-3624iF only).
- RS-232 DCE console port for diagnosing the Switch via a connection to a PC and Console/Out-of-band management (DES-3624i or DES-3624iF only).
- One slide-in module interface in the front panel for 1 or 2 ports 10/100M Ethernet connection. Three optional modules are available: 2-port TX, 2-port FX (MT-RJ), and 1-port FX (SC).
- Stacking Input/Output port slide-in module in the rear panel for stacking to another device to implement a high-port count, manageable switch. Three-port module for master device and one-port module for a client device.

Performance features

- Store and forward switching scheme capability to support rate adaptation and protocol conversion.
- Full and half-duplex for 10Mbps and 100Mbps connections. The 1000BASE-SX module operates at full-duplex only. Full-duplex allows the switch port to simultaneously transmit and receive data, and only works with connections to full-duplex capable end stations and switches. Connections to hubs must take place at half-duplex.

- Auto polarity detection and correction of incorrect polarity on the receive twisted pair at each port.
- Data forwarding rate 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data forwarding rate 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- Data forwarding rate 1,488,100 pps per port at 100% of wire-speed for 1000Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 1,488,100 pps per port at 100% of wire-speed for 1000Mbps speed.
- 12K active MAC address entry table per device with automatic learning and aging (10 to 9999 seconds).
- 12 MB packet buffer per device.
- Supports Broadcast Storm filtering.
- Supports IGMP Multicast snooping.

Management

- RS-232 console port for out-of-band network management via a console terminal or PC.

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

2

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Switch.

Unpacking

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

- One Stackable NWay Ethernet Switch
- Mounting kit: two mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This user's guide on CD-ROM with a Registration Card

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

Setup

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

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

Desktop or Shelf Installation

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

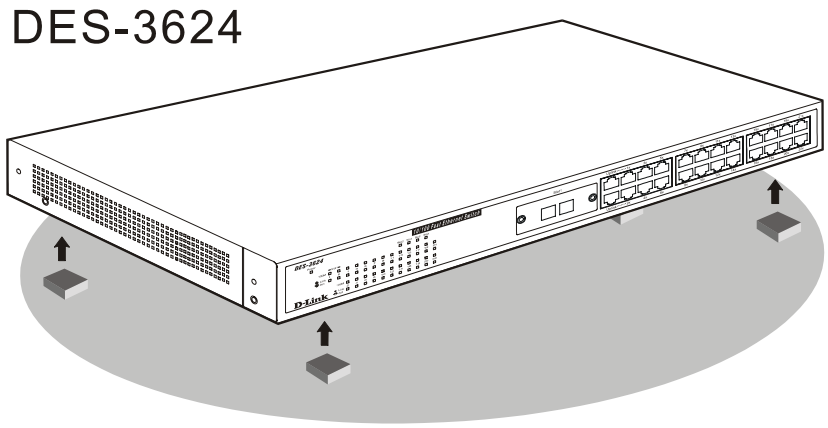


Figure 2-1. Switch installed on a Desktop or Shelf

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.

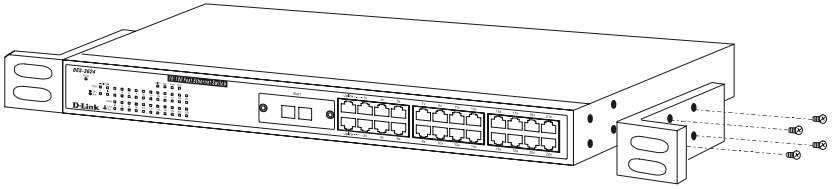


Figure 2-2A. Attaching the mounting brackets to the Switch

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

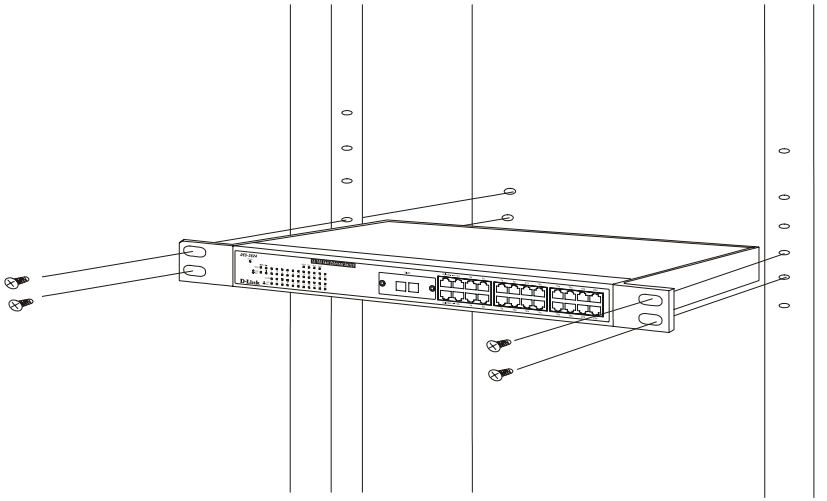


Figure 2-2B. Installing the Switch in an equipment rack

Power on

The Switch can be used with AC power sources 100 - 240 VAC, 50 - 60 Hz. The power switch is located at the rear of the unit adjacent to the AC power connector and the system fan. The Switch's power supply will adjust to the local power source automatically and may be turned on without having any or all LAN segment cables connected.

After the power switch is turned on, the LED indicators should respond as follows:

- All LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.
- The power LED indicator will blink while the Switch loads onboard software and performs a self-test. After approximately 40 seconds, the LED will light continuously to indicate the Switch is in a ready state.
- The console LED indicator will remain ON if there is a connection at the RS-232 port, otherwise this LED indicator is OFF.
- The 100M LED indicator may remain ON or OFF depending on the transmission speed.

Power Failure

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

3

IDENTIFYING EXTERNAL COMPONENTS

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

Front Panel

The front panel of the Switch consists of either 19 or 20 (10/100 Mbps) Ethernet/Fast Ethernet ports, one or two uplink jacks, a slide-in module slot for 10/100 Mbps Ethernet ports, an RS-232 communication port (DES-3624i and DES-3624iF only), and LED indicators.

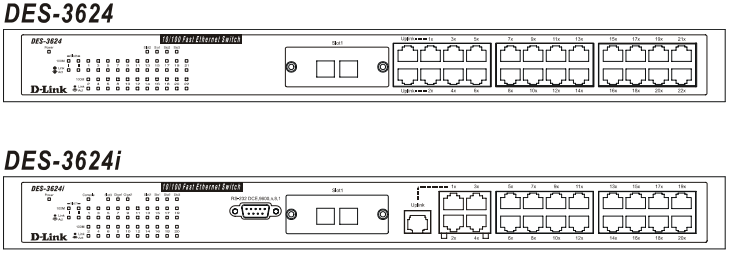


Figure 3-1. Front panel view of the Switches

- 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 PC and Local Console Management (DES-3624i and DES-3624iF only).
- Nineteen or 20 high performance NWay ports all operate at 10/100 Mbps for connection to servers and hubs. All ports can be auto-negotiated between 10Mbps or 100Mbps.
- A slide-in module slot (labeled Slot1) for 10/100 Mbps Ethernet ports can accommodate the following modules: 2-port TX, 2-port FX (MT-RJ), or 1-port FX (SC).
- One or two MDI-II uplink jacks are supported. Port numbers 1 and 2 on the DES-3624 and the DES-3624F are equipped with MDI-X jacks for normal end-node connections and MDI-II jacks for uplink connections. Port number 1 on the DES-3624i and DES-3624iF are equipped with an MDI-X jack for normal end-node connection and an MDI-II jack for uplink connection.

Rear Panel

The rear panel of the DES-3624 and the DES-3624F consist of a slot (labeled Slot2) for a Stacking input/output port and an AC power connector. The rear panel of the DES-3624i and DES-3624iF consist of two slots (labeled Slot2 and Slot3). Slot2 is for Stacking input/output ports Sio1, Sio2, and Sio3. Slot3 is for an optional Gigabit Ethernet uplink (MDI-II) port. The following shows the rear panel of the Switches.

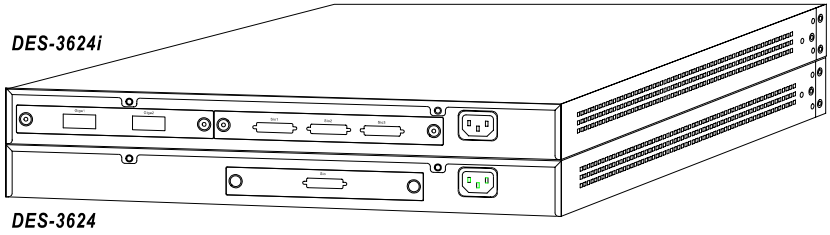


Figure 3-2. Rear panel view of the Switches

- The optional Gigabit Ethernet slide-in module is an uplink/MDI-II (media dependent interface) port for uplink to another Switch (DES-3624i and DES-3624iF only). Two models are available, one-port and two-port.

- The Stacking input/output port slide-in module in the rear panel is for stacking to another device to implement a high-port count, manageable Switch. The three-port module is for a master device and a one-port module is for a client device.

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

Side Panels

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

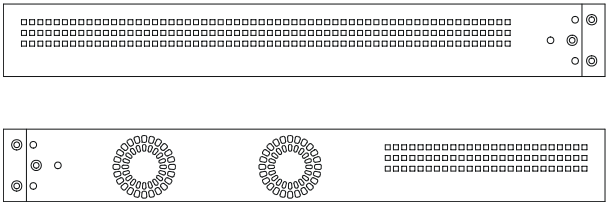


Figure 3-3. Side panel views of the Switch

- The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave 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.

Stack Operation

The DES-3624i and the DES-3624iF are intelligent Switches capable of acting as a master for up to three client Switches (DES-3624 and DES-3624F). Each port is referred to by unit ID and port number in your DES-3624 Series stack.

To set up a stack, a one-port Stacking input/output module is needed for each client Switch and a three-port Stacking input/output module is needed for the master Switch. Once the modules have been installed, use a cascade cable to connect each client Switch to the master Switch.

Figure 3-4. Switch stack with one master and three clients

Please note that two client switches can also be connected via the Stacking input/output ports.

The following diagram displays some possible switch stack connections:

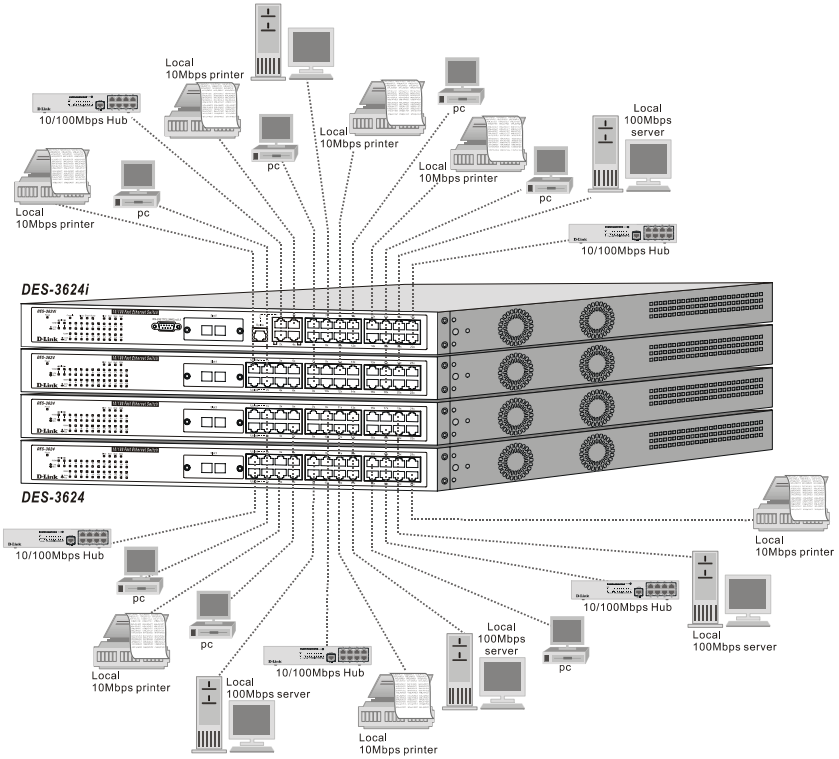


Figure 3-5. Switch stack with example of possible connections

Optional Plug-in Modules

The DES-3624i/DES-3624iF Stackable NWay Ethernet Switch is able to accommodate a range of plug-in modules in order to increase functionality and performance.

100BASE-FX (MT-RJ) Module

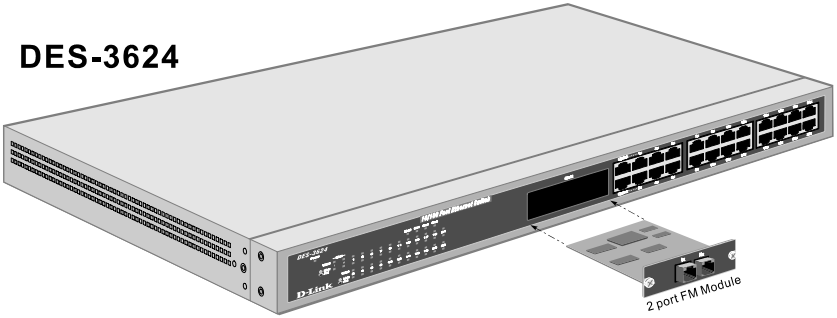


Figure 3-6. Two-port, 100BASE-FX (MT-RJ) module

- Two-port, front-panel module.
- Connects to 100BASE-FX devices at full- or half-duplex.
- Supports multi-mode fiber-optic cable connections of up to 412 meters in half-duplex or 2 km in full-duplex mode.

100BASE-FX (SC) Module

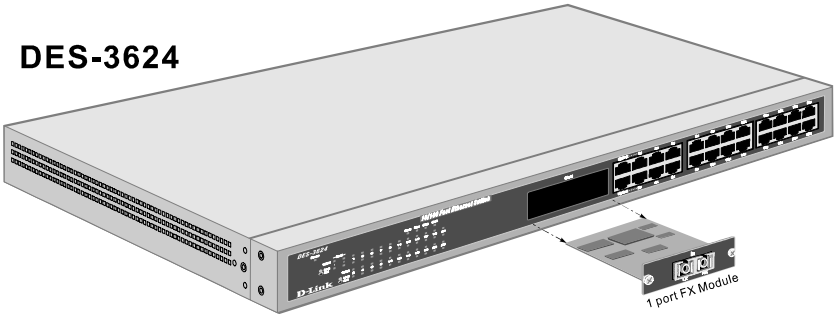


Figure 3-7. One-port, 100BASE-FX (SC) module

- One-port, front panel module.
- Connects to a 100BASE-FX device at full- or half-duplex.
- Supports multi-mode fiber-optic cable connections of up to 412 meters in half-duplex or 2 km in full-duplex mode.

100BASE-TX Module

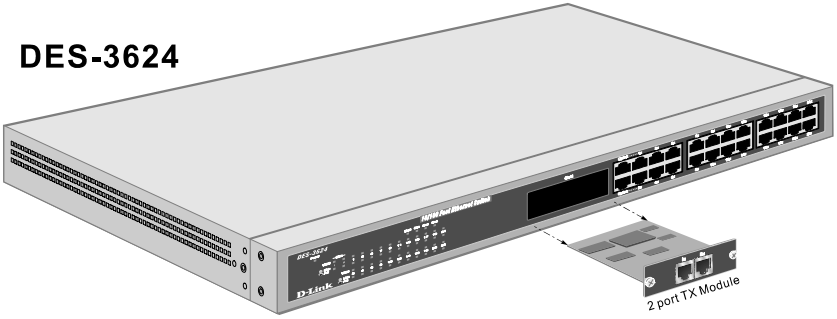


Figure 3-8. Two-port, 100BASE-TX module

- Two-port, front-panel module.
- Connects to 100BASE-TX devices at full or half duplex.
- Supports Category 5 UTP or STP cable connections of up to 100 meters.

1000BASE-SX Gigabit Module

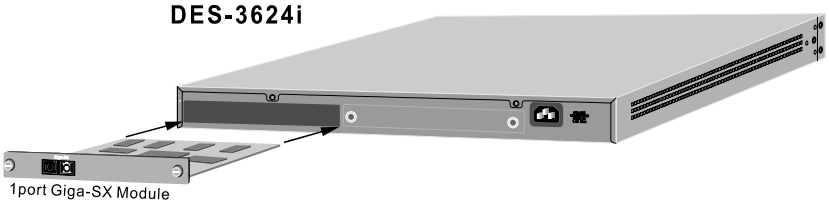


Figure 3-9. One-port, 1000BASE-SX gigabit module

- One- or two-port, rear-panel module.
- Connects to 1000BASE-SX devices at full duplex.
- Allows connections using multi-mode fiber optic cable in the following configurations:

	62.5μm	**62.5μm**	**50μm**	**50μm**
Modal bandwidth (min. overfilled launch) Unit: MHz*km	160	200	400	500
Operating distance Unit: meters	220	275	500	550
Channel insertion loss Unit: dB	2.33	2.53	3.25	3.43

1000BASE-LX Gigabit Module

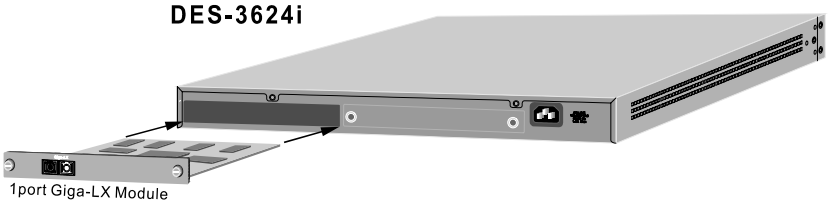


Figure 3-10. One-port, 1000BASE-LX gigabit module

- One-port, rear-panel module.
- Connects to a 1000BASE-LX device at full duplex.
- Allows connections up to 5 km in length using single-mode fiber optic cable.

LED Indicators

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

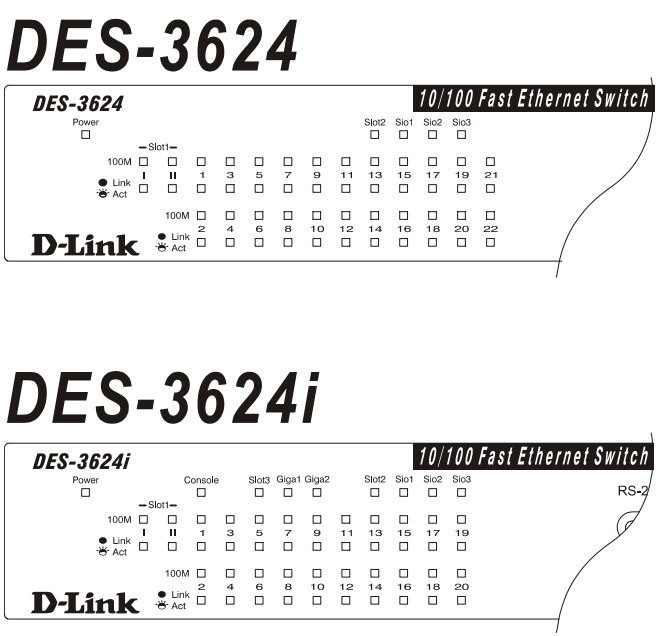


Figure 3-11. The Switch LED indicators

- **Power** This indicator on the front panel should light green after approximately 2 seconds to indicate the ready state of the Switch when the device is powered on. The LED will blink when the Power-On Self-Test (POST) is running or if the system's configuration has changed. This LED will light orange when an error occurs.

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

- **Slot2** This indicator is lit green when a slide-in module is present in the rear panel of the Switch.
- **Slot3** This indicator is lit green when a slide-in module is present in the rear panel of the Switch.
- **Giga1** This indicator is lit green when a link is established. It blinks green when the Gigabit port is active.
- **Giga2** This indicator is lit green when a link is established. It blinks green when the Gigabit port is active.
- **Sio1** This indicator is lit green when a Stacking IO port is present in the rear panel of the Switch.
- **Sio2** This indicator is lit green when a Stacking IO port is present in the rear panel of the Switch.
- **Sio3** This indicator is lit green when a Stacking IO port is present in the rear panel of the Switch.
- **100M** These indicators are illuminated green when a 100 Mbps device is connected to any of the 22+2 or 20+2 ports or uplink port. If a 10 Mbps device is connected to any of the 24 ports or uplink port, these LEDs remain dark. When a port is active, these indicators will blink green.
- **Link/Act** These indicators are lit when there is a secure connection (or link) to a device at any of the ports. The LEDs blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.

4

CONNECTING THE SWITCH

This chapter describes how to connect the Switch to your Ethernet network.

Switch to End Node

End nodes include PCs outfitted with a 10, 100 or 10/100 Mbps RJ-45 Ethernet/Fast Ethernet Network Interface Card (NIC) and most routers. 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 100 Mbps Fast Ethernet connections). The end node should be connected to any of the twenty-two ports (1x - 22x) of the Switch or to either of the two 100BASE-TX ports on the front-panel module that came preinstalled on the Switch. An end node should not be connected to an Uplink port (unless using a crossover cable), and if the top Uplink port is in use, Port 1x must remain vacant; if the bottom Uplink port is in use, Port 2x cannot be used.

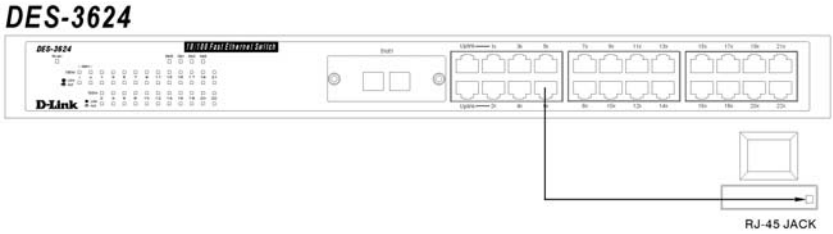


Figure 4-1. Switch connected to an End Node

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 LED indicator comes *ON* for a 100 Mbps and stays *OFF* for 10 Mbps.

2. The Link/Act LED 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. 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 must be made from Uplink to Uplink, or from a 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 - 22x, or one of the 100BASE-TX module ports) using a normal straight-through cable, as shown below.

If the other device does not have an unused Uplink port, make the connection with a normal straight-through cable from one of the Uplink ports on the switch to any normal crossed port on the hub. Alternatively, if you have a crossover cable you can save the Uplink ports for other connections and make this one from a crossed port to another crossed port.

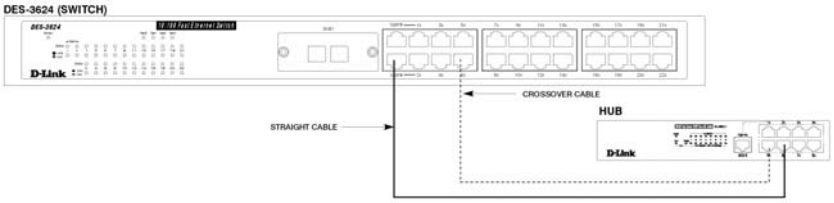


Figure 4-2. Switch connected to a normal (non-Uplink) port on a hub or switch using a straight or crossover cable

10BASE-T Device

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

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

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 D-View, 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). You can change the default Switch 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.

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 STA specifications. Each 10Mbps and 100Mbps segment has an assigned Path Cost of 19.

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*.

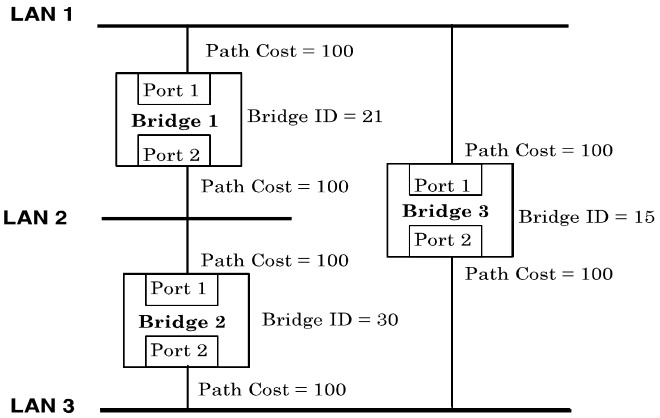


Figure 5-1. Before Applying the STA Rules

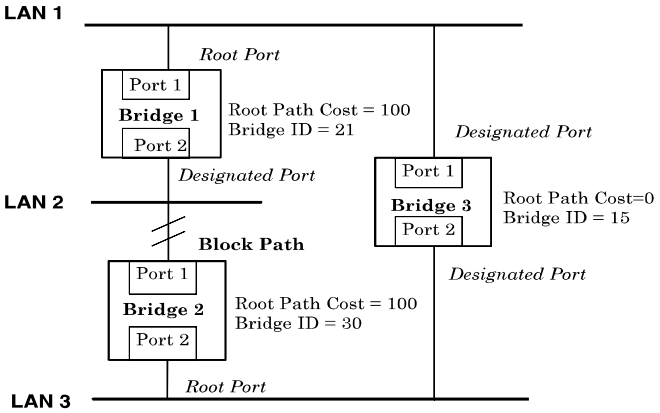


Figure 5-2. After Applying the STA Rules

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 3 trunk groups, which may include from 2 to 8 switch ports each, except for the third trunk group which consists of the 2 ports of the Slot 1, 100BASE-TX or

100BASE-FX front-panel module. The anchor port for the first group is preset as port 5, the anchor port for the second group is port 13 and the anchor port for the third group is the first port (1x) on the 2-port module.

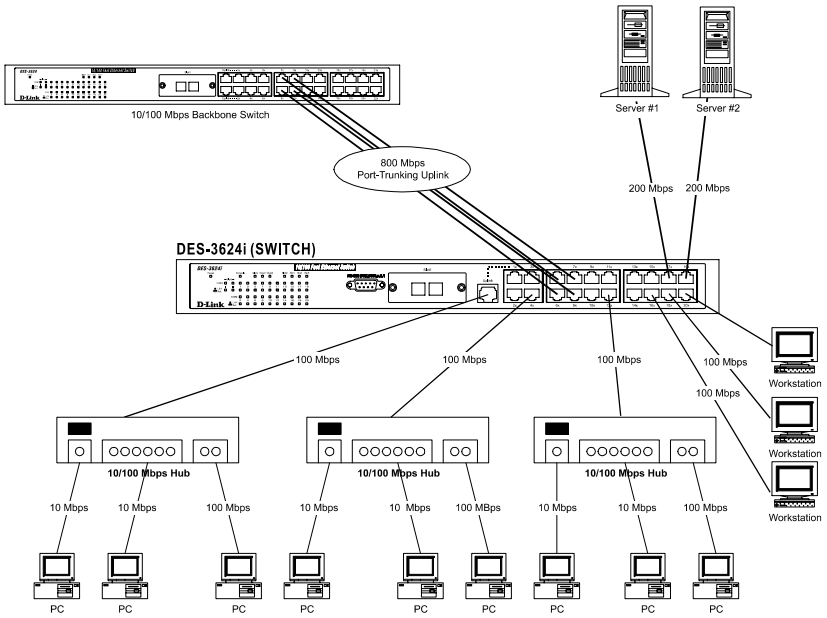


Figure 5-3. Port trunking example

The switch treats all ports in a trunk group as a single port. As such, trunk ports will not be blocked by Spanning Tree (unless a redundant link with higher STP priority is present).

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. A trunk connection cannot be made with switches that perform load-balancing on a per-packet basis.

VLAN

VLANs are a collection of switch ports grouped together in a secure, autonomous broadcast and multicast domain. VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All Ethernet packets (unicast, broadcast, multicast, unknown, etc.) entering a VLAN will only be forwarded to the ports that are members of that VLAN.

Another benefit of VLANs is that you can change the network topology without physically moving stations or changing cable connections. Stations can be "moved" simply by changing 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.

VLANs can also provide a level of security to your network. Port-based VLANs allow you to configure ports to not send or receive packets outside of the VLAN.

The *untagging* feature of IEEE 802.1Q VLANs allow 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.

IEEE 802.1Q VLANs

The Switch supports up to 96 IEEE 802.1Q (port-based) VLANs. Port-based 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 port-based 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 IEEE 802.1Q VLANs; Port VLAN ID numbers (PVID) and VLAN ID numbers (VID). 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 switch will forward packets from the connected segment on, 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.

VLAN Segmentation

Take for example 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 it's 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 VLANs

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

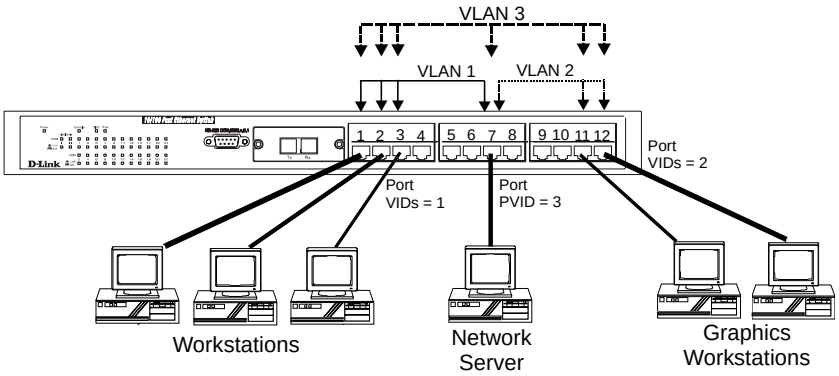


Figure 5-4. Example of typical VLAN configuration

In the above example, there are three different 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:

Transmit on VLAN #			Member of VLAN #	
Port	**PVID**		**VID**	**Ports**
Port 1	1		1	1,2,3,7
Port 2	1			
Port 3	1			
Port 7	3		3	1,2,3,7,11, 12
Port 11	2		2	11,12,7
Port 12	2			

Table 5-2. Example of possible VLAN assignments

The server attached to Port 7 is shared by VLAN 1 and VLAN 2 because Port 7 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 to be printed. Ports 1, 2 and 3 send these packets on VLAN 1 (their PVID=1), and Ports 11 and 11 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).

VLANs Spanning Multiple Switches

VLANs can span multiple switches as well as your entire network. Two considerations to keep in mind while building VLANs of this sort are whether the switches are IEEE 802.1Q-

compliant and whether VLAN packets should be tagged or untagged.

Definitions of relevant terms are as follows:

- **Tagging** The act of putting 802.1Q VLAN information into the header of a packet. Ports with tagging enabled will put the VID number, priority, and other VLAN information into all packets that flow 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. Ports with untagging enabled 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 and VLAN decisions must be made. Basically, the switch examines VLAN information in the packet header (if present) and decides whether to forward the packet. If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN and can thus receive the packet (if the Ingress Filter is enabled), and then it decides if the destination port is a member of the VLAN. Assuming both ports are members of the tagged VLAN, the packet will be forwarded. If the packet doesn't have VLAN information in its header (is untagged), the ingress port first determines if the ingress port itself can receive the packet (if the Ingress Filter is enabled), will tag it with its own PVID (if it defined as a tagging port), and check to see if the destination port is on the same VLAN as its own PVID and can thus receive the

packet. If Ingress filtering is disabled and the destination port is a member of the VLAN used by the ingress port, the packet will be forwarded. If the ingress port is an untagging port, it will only check the filter condition--if the filter condition is enabled-- before forwarding the packet.

- **Egress port** A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made. If an egress port is connected to an 802.1Q-compliant switch, tagging should be enabled so the other switch can take VLAN data into account when making forwarding decisions. 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.

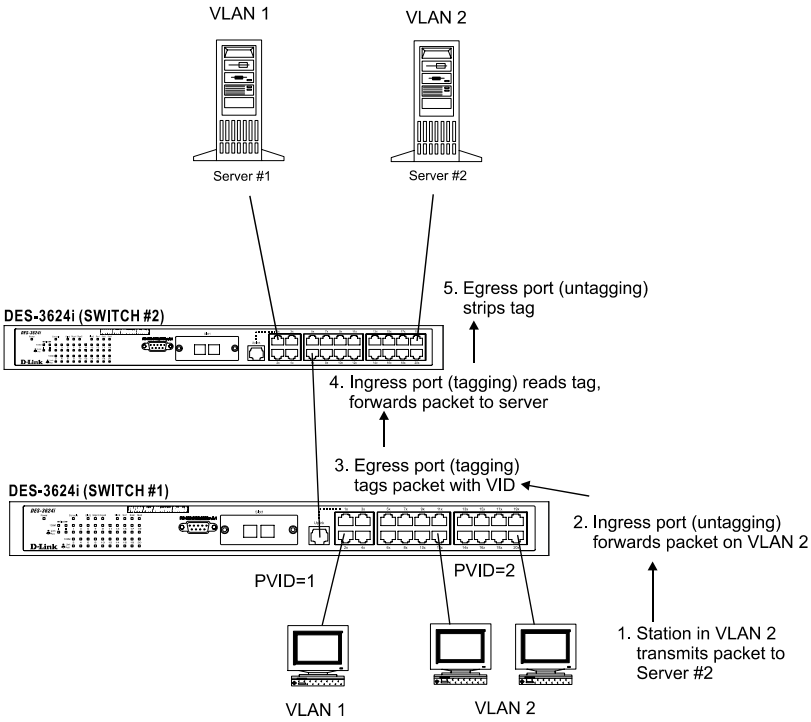


Figure 5-5. Data transmissions between 802.1Q-compliant Switches

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

If the ingress port in step 4 were connected to a non-802.1Q-compliant device and was thus receiving untagged packets, it would tag its own PVID onto the packet and use this

information to make forwarding decisions. As a result, the packets coming from the non-compliant device would automatically be placed on the ingress ports VLAN and could only communicate with other ports that are members of this VLAN.

Broadcast Management

Broadcast transmissions, packets sent to every devices on the LAN, are a vital part of any network. However, they can often cause problems on the network and even network failure. For this reason the Switch has a number of tools for managing broadcast packets on your network.

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. Some of the causes of broadcast storms are network loops, malfunctioning NICs, bad cable connections, and applications or protocols that generate broadcast traffic.

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, limit their scope. However, switches are now able to limit broadcast domains better and cheaper than routers. Also, many switches have broadcast sensors and filters built into each port to further control broadcast storms—such as the Switch you have purchased.

Port-based Broadcast Packet Filter

The Switch is equipped with sensors that count the number of broadcast frames arriving at each port. When a certain level (*rising threshold*) is reached, the sensors can initiate a broadcast filter (*rising action*) which drops all broadcast packets arriving at the affected port. This effectively partitions the broadcast packets from the rest of the network, thereby limiting the effects of a broadcast storm. The port-based Broadcast Storm Filter settings can be set by the user. Please refer to the **Configure Ports** section of this manual for more detailed explanations regarding port-based Broadcast Storm filter settings.

MAC-based Broadcast Packet Filter

Broadcast domains can also be managed on the MAC level. In this case, broadcast domains can be defined to include specific devices (MAC addresses). To do this, simply enter the MAC addresses of the computers and peripherals you wish to include in the broadcast domain(s). Any unknown or broadcast packets generated within the Mac-based broadcast domain will only be sent to the other members. Other parts of the network are effectively shielded. Configuring MAC-based broadcast domains is done in the **VLANs and MAC-based Broadcast Domains** submenus of the Console or Web-based management programs.

6

USING THE CONSOLE INTERFACE

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

Connecting to the Switch

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

- VT-100/ANSI compatible

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

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

Console Usage Conventions

The console interface makes use of the following conventions:

1. Items in **<***angle brackets***>** can be toggled on or off using the space bar.
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.

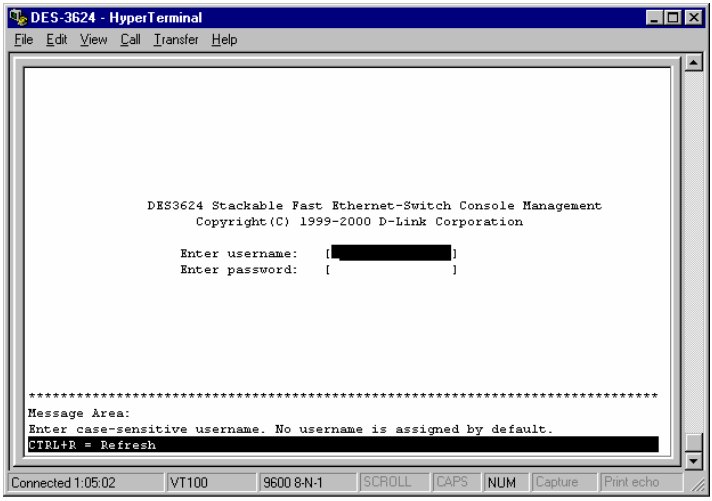


Figure 6-1. Initial Screen, first time connecting to the Switch

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

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

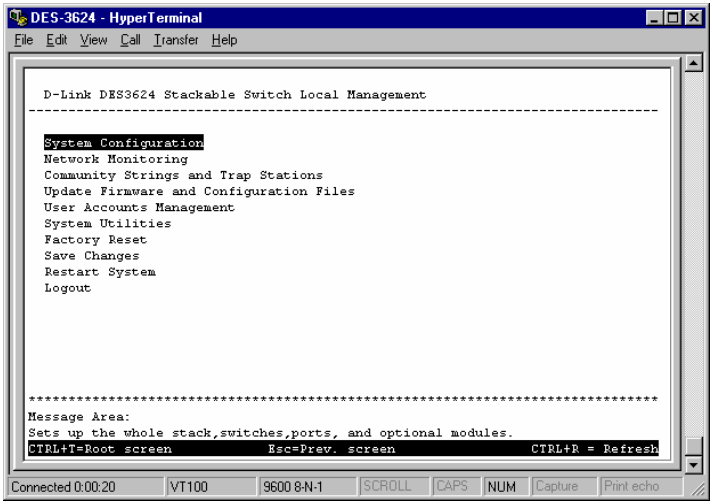


Figure 6-2. Main Menu

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

User Accounts Management

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	Yes	Yes, view only.
Network Monitoring	Yes	Yes, view only.
Community Strings and Trap Stations	Yes	Yes, view only.
Update Firmware and Configuration Files	Yes	Yes, view only.
User Accounts Management		
Create/Modify User Accounts	Yes	Yes, view only.
View/ Delete User Accounts	Yes	Yes, view only.
System Utilities	Yes	Yes, (Ping Test); view only for the rest.
Factory Reset	Yes	No
Restart System	Yes	No

Table 6-1. Administrator and Normal User Privileges

After establishing a User Account with **Administrator**-level privileges, press Esc. twice. Then choose the **Save Changes** menu (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:

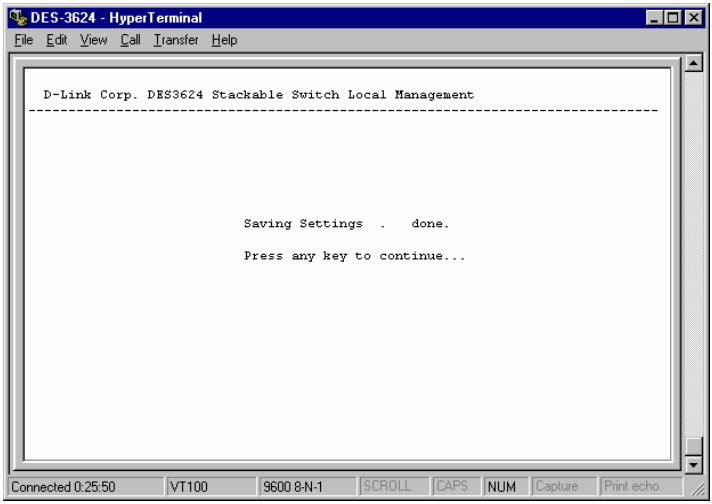


Figure 6-3. Save Changes screen

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 Appendix D, 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:

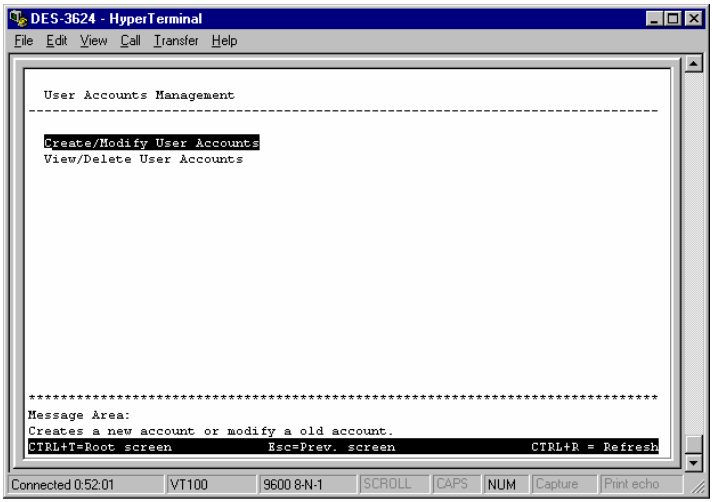


Figure 6-4. User Accounts Management menu

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

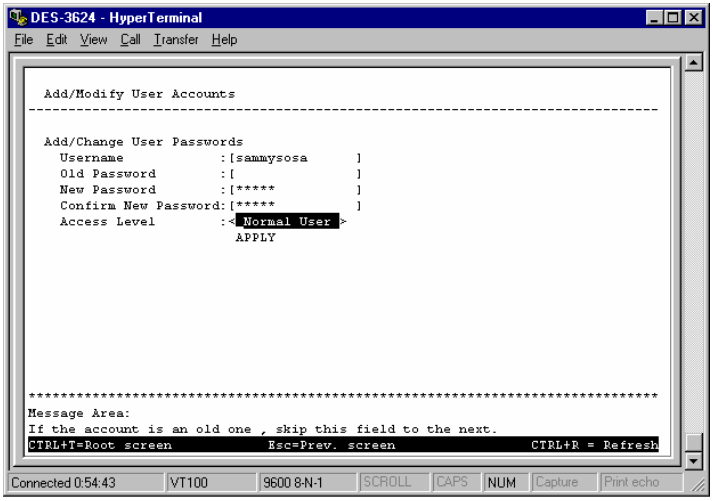


Figure 6-5. Add/Modify User Accounts screen

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.

View/Delete User Accounts

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

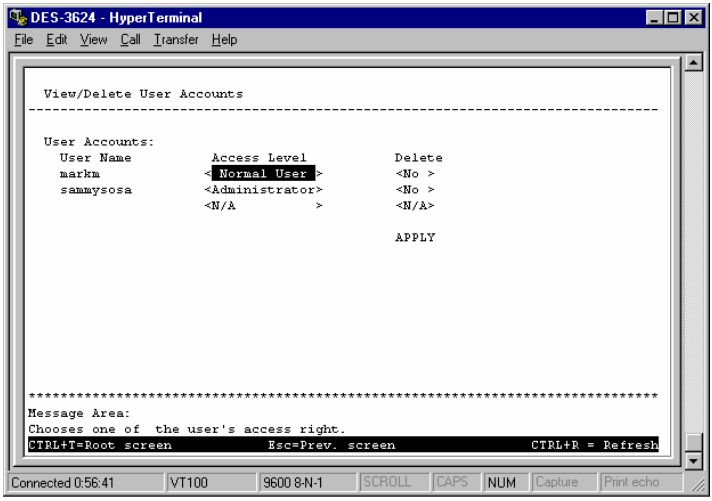


Figure 6-6. View/Delete User Accounts screen

To delete your user password:

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

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

Setting Up The Switch

This section will help prepare the Switch user by describing the **System Configuration**, **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:

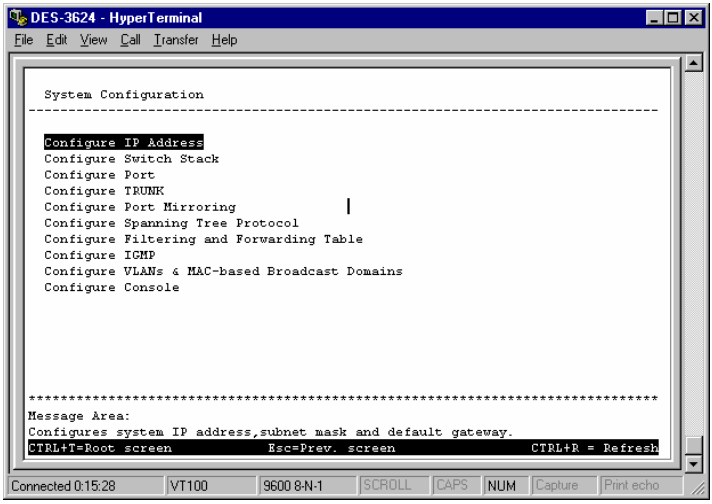


Figure 6-7. System Configuration menu

You will need to change some settings to allow you to be able to manage the Switch from an SNMP-based Network Management System such as SNMP v1 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 or Telnet client 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:

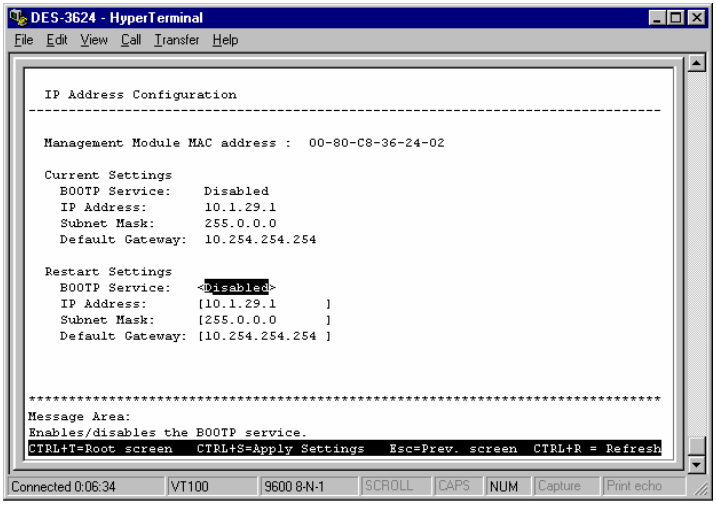


Figure 6-8. IP Address Configuration screen

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 reset. Fields that can be set include:

- **BOOTP Service** Determines whether the Switch should send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned on a central BOOTP server; if this option is set the Switch will first look for a BOOTP server to provide it with this information before using the supplied settings.

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

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

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

Configure Console

You can use the **Console Options** screen to choose whether to use the Switch's RS-232C serial port for console management or for out-of-band TCP/IP communications using SLIP, and to set the bit rate used for SLIP communications. Note that the DES-3624i has an RS-232C serial port but the DES-3624 does not.

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

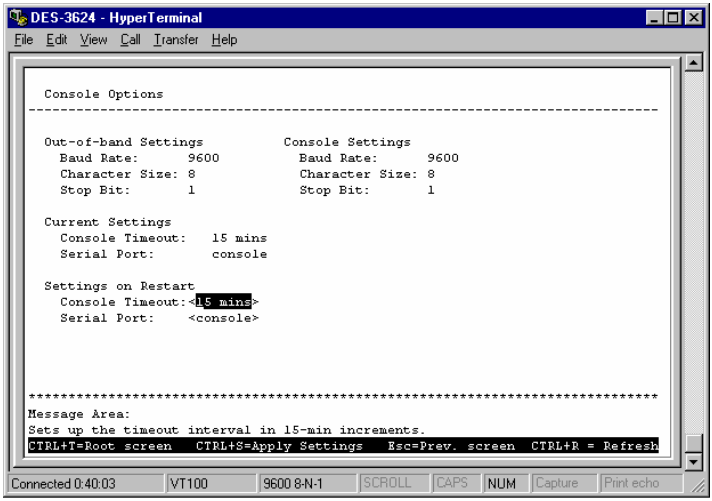


Figure 6-9. Console Options screen

The following fields can be set:

Settings on Restart:

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

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

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

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

Configure Switch Stack

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

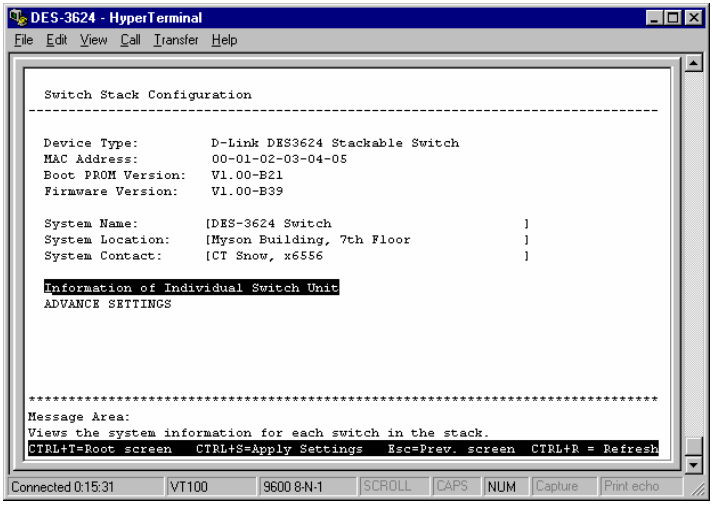


Figure 6-10. Switch Stack Configuration screen

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.

Information of Individual Switch Unit

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

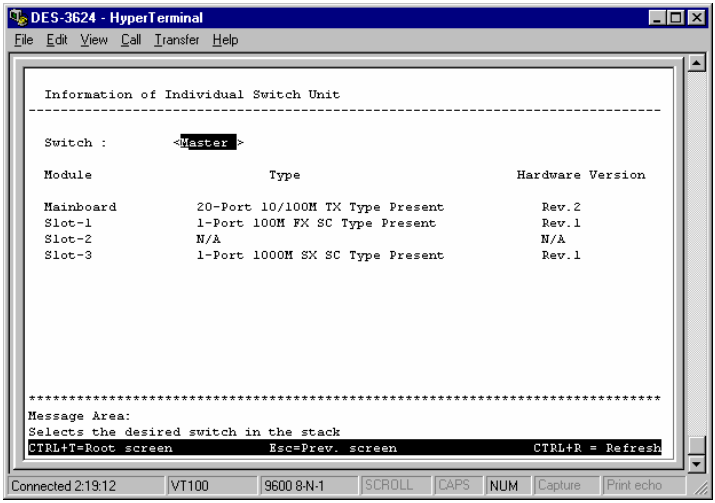


Figure 6-11A. Information of Individual Switch Unit screen

Use the space bar to select the desired Switch in your stack. For example, if there were two Switches, the master would look like the screen above and the client would look like the screen below:

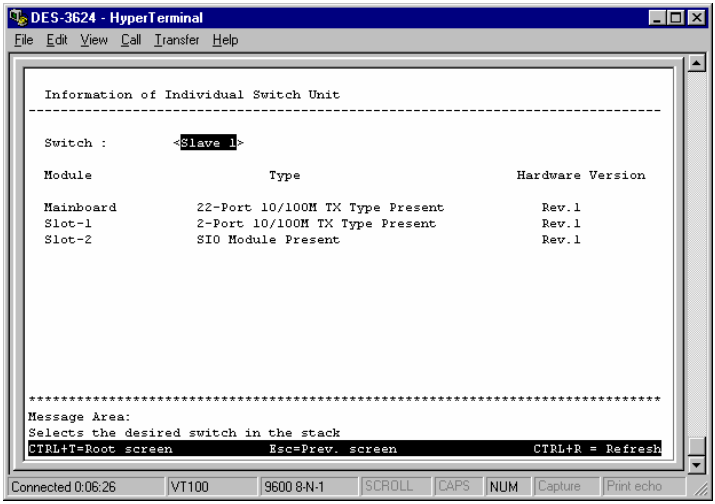


Figure 6-11B. Information of Individual Switch Unit screen

Advance Settings

The **Configure Advanced Switch Features** screen allows you to set an expiration time for MAC address entries and enable or disable auto-partitioning on all ports. Press ADVANCE SETTINGS on the **Switch Stack Configuration** screen to access the **Configure Advanced Switch Features** screen:

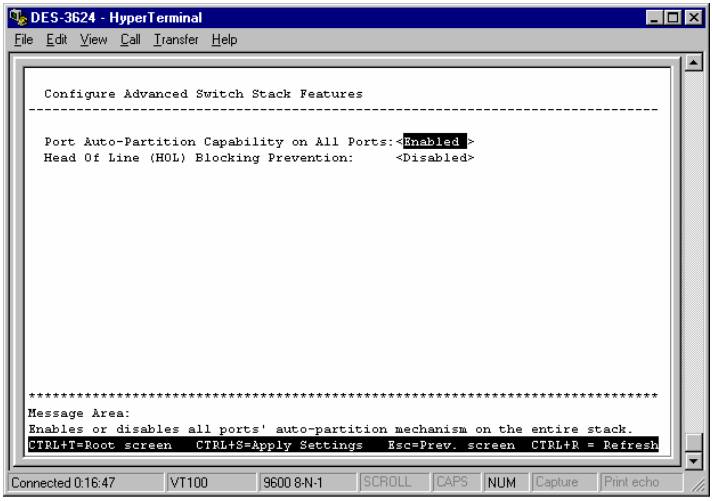


Figure 6-12. Configure Advanced Switch Features screen

The fields you can set are:

- **Port Auto-Partition Capability on All Ports** When this function is enabled, if too many consecutive collisions occur on an individual port, the port will be blocked off until a good packet is seen on the wire. If a port is partitioned, the Switch can only transmit data, not receive it.

- **Head Of Line (HOL) Blocking Prevention** *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 the port 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 Port

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

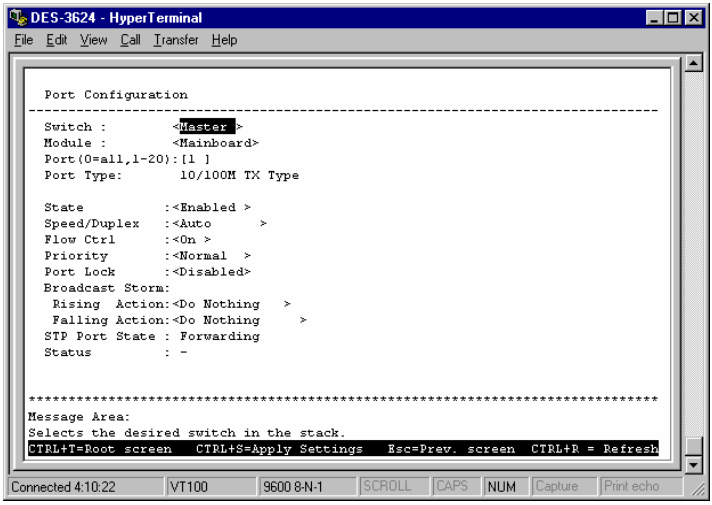


Figure 6-13. Port Configuration screen

Items in the above window are defined as follows:

- **Switch** Specifies the Switch where the port is being configured.
- **Module** Specifies the module where the port is being configured.
- **Port** Specifies the port that will be configured.

- **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*. If a Gigabit module is being used, *1000M/Full* will be displayed in this field. Choosing *Auto* enables NWay auto-configuration on the port.

- **Flow Ctrl** Toggles flow control *On* or *Off*. It 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. Confirm that Flow Control is in force by checking the **Status** field.

- **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 *Blocking-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. *Blocking-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 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 *Forwarding-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*. *Forwarding-Trap* performs the same action as *Forwarding*, except it also sends a trap to the designated Trap Recipient informing them of the situation.

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

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

Configure Trunk

Ports on the Switch can be grouped together in a single logical port called a trunk. This is discussed in detail in the *Port Trunking* section of the "Switch Management Concepts" chapter of this manual.

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

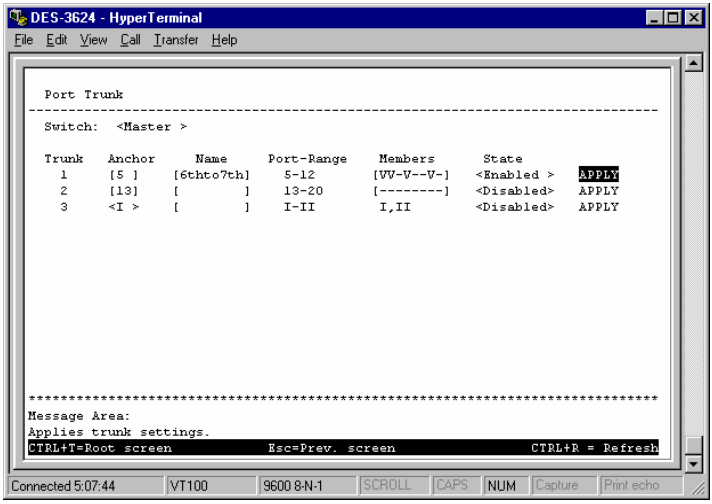


Figure 6-14. Port Trunk screen

The fields you can set are:

- **Anchor** There are either two or three listings representing the anchor port for each of the three trunk groups available on the Switch (the third listing will only be displayed if an optional two-port plug-in module is being used). 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 between a Switch on the 6th floor and this one on the 7th floor

- **Members** Select between 2 to 8 ports in the first two entries for this field. The number of ports defined here start from the anchor port. Thus, in the example pictured above containing 4 ports in the first trunk, the ports in the trunk group will include ports (anchor), 5, 6, 8, and 11. The third entry (used for 2-port front-panel modules) has a permanent setting of 2 ports.

- **State** *Enabled*, *Disabled* or *Clear*. Be careful when clearing trunk groups as the connections will return to normal operation and may cause signal loops.

Port Range is a read-only field which lists the possible ports in a selected trunk.

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:

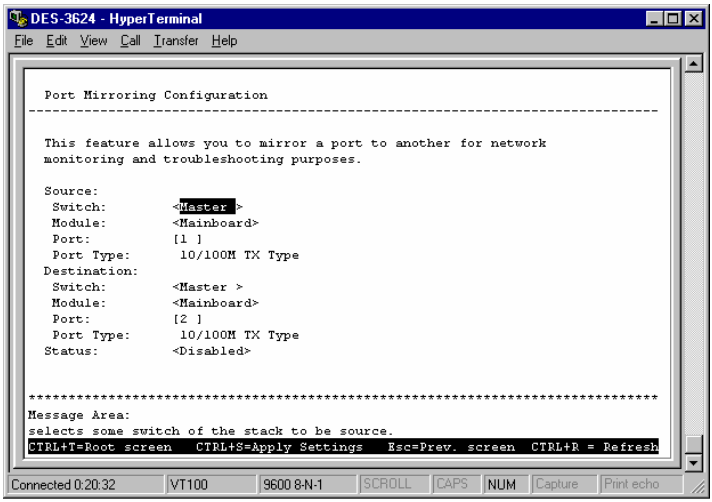


Figure 6-15. Port Mirroring Configuration screen

To configure a mirror port, select the **Switch**, **Module**, and **Port** from where you want to copy frames in the **Source** fields. Then select the **Switch**, **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 cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to

which you are sending the copies. Also, the target port cannot be a member of a trunk group.

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:

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

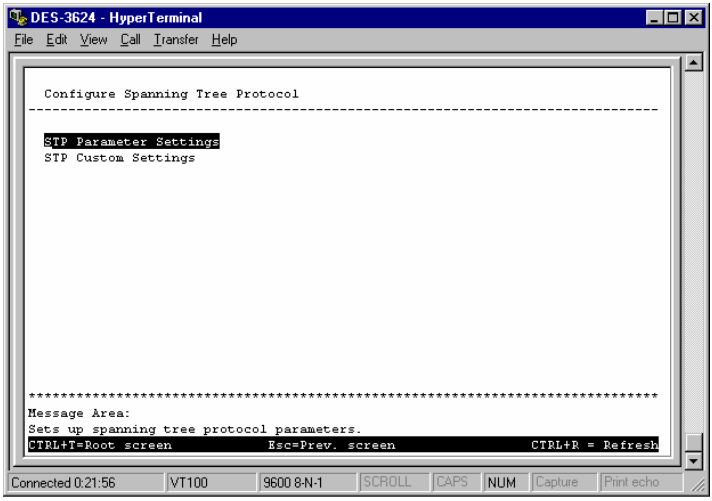


Figure 6-16. Configure Spanning Tree Protocol menu

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

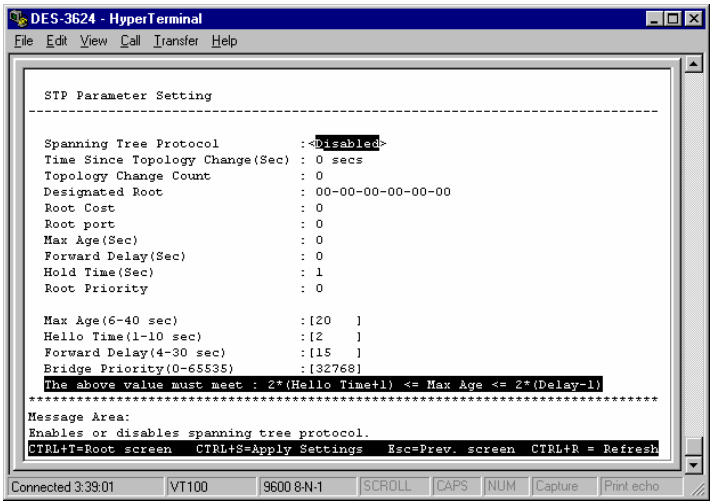


Figure 6-17. STP Parameter Setting screen

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

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

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

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

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

The information on the screen is described as follows:

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

- **Time Since Topology 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 multibridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. A bridge priority ranges from 0 to 65535, with 0 being the highest priority.

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

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

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

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

STP Custom Settings

To change the parameters on individual ports:

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

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

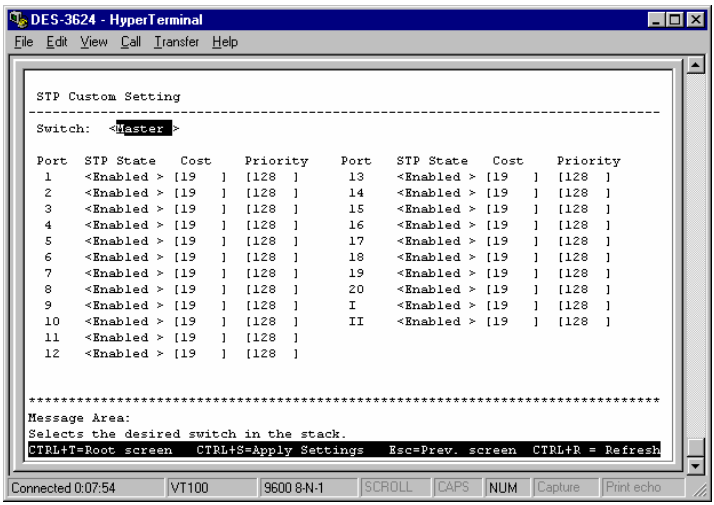


Figure 6-18. STP Custom Settings screen

Items in the above window are described as follows:

- **STP State** Sets the Spanning Tree Protocol on a particular port to *Enabled or Disabled*.

- **Cost** Defines the cost for the connection.

- **Priority** Port Priority is a read-write object that can be set from 0 to 255. This is the priority number of the

port. The higher the port priority, the more chance the bridge has of becoming the root 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.

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 address learning, change the way the Switch treats MAC address table entries, and select an age-out time of the MAC address in the selected address 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:

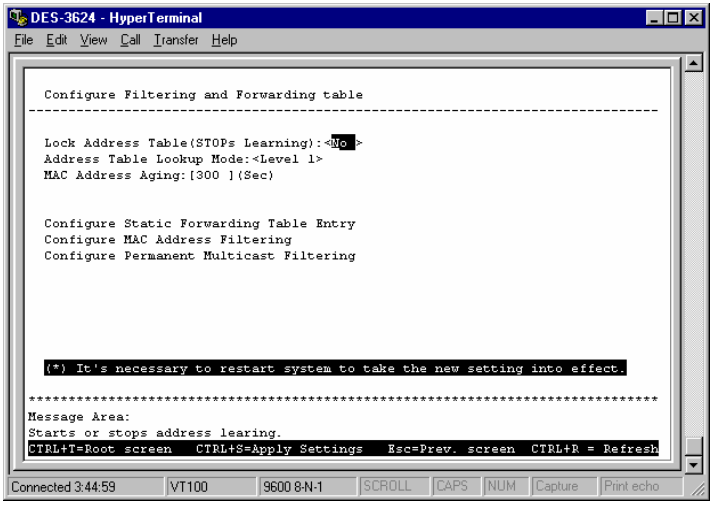


Figure 6-19. Configure Filtering and Forwarding table screen

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

- **Lock Address Table(STOPs Learning)** 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 coming from an unknown source address will be dropped by the Switch.

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

- **MAC Address Aging** 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 Entry

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

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 Entry** from the bottom of the **Configure Filtering and Forwarding table** screen. The following screen appears:

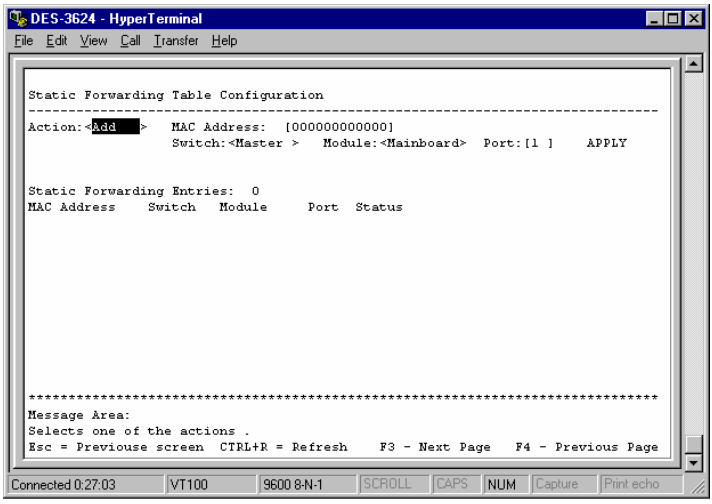


Figure 6-20. Static Forwarding Table Configuration screen

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.
- **Switch**, **Module**, and **Port** The Switch, module, and port number are entered in these fields at the top of the screen. The Switch will always forward traffic to the specified device through this port. The bottom of the screen will display each corresponding destination address for these three items.

Status is a read-only field which lists 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 **Custom Filtering Table** contains filtering information configured into the Switch by (local or network) management specifying destination 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 **Custom 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:

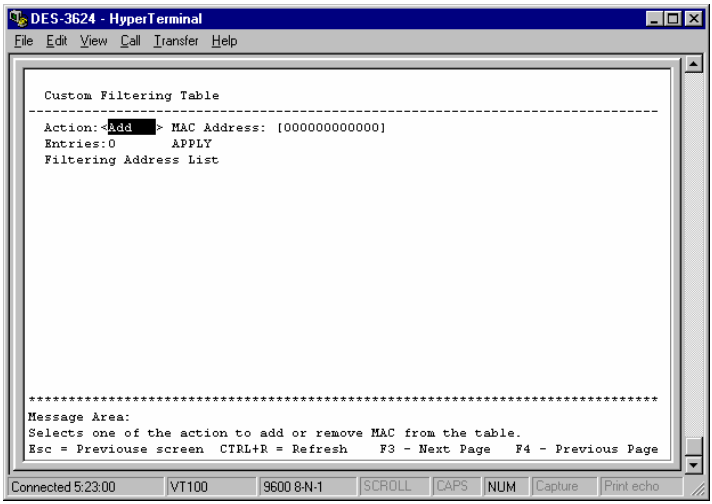


Figure 6-21. Custom Filtering Table screen

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

Configure Permanent Multicast Filtering

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

To access the **Static Multicast Filtering Table Configuration** screen, select **Configure Filtering and Forwarding Table** from the **System Configuration** menu. Then select **Configure Permanent Multicast Filtering** from the bottom of the

Configure Filtering and Forwarding table screen. The following screen appears:

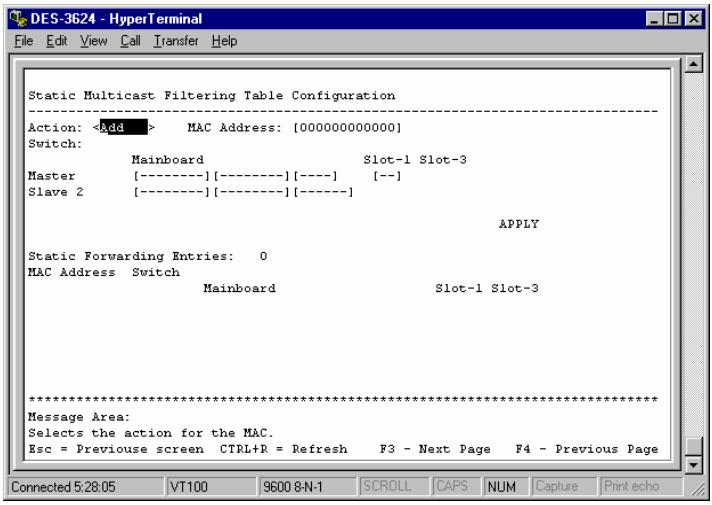


Figure 6-22. Static Multicast Filtering Table Configuration screen

To make a change to the **Static Multicast Filtering Table**, choose *Add* or *Remove* in the **Action** field. Then enter the **MAC Address** and the member port numbers in the desired fields, for example **Master** and **Slave 1** if there are two Switches in your stack. 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.

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:

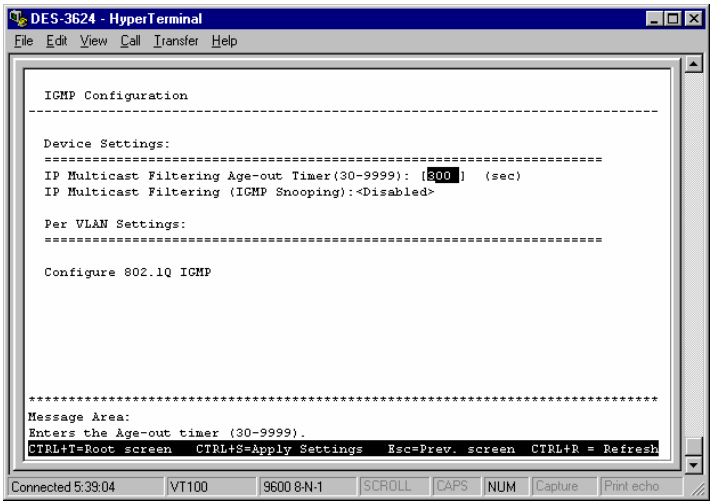


Figure 6-23. IGMP Configuration screen

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 contains a command for VLAN settings that leads to the **IEEE 802.1q IGMP Configuration** menu. Highlight **Configure 802.1Q IGMP** and press Enter to access this screen:

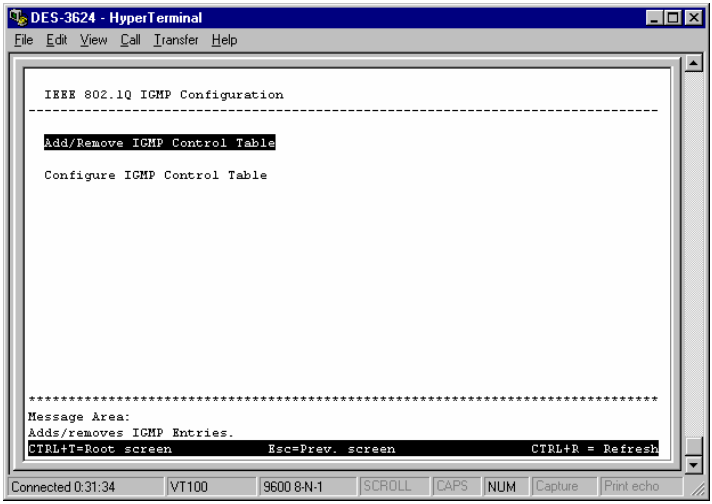


Figure 6-24. IEEE 802.1q IGMP Configuration screen

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

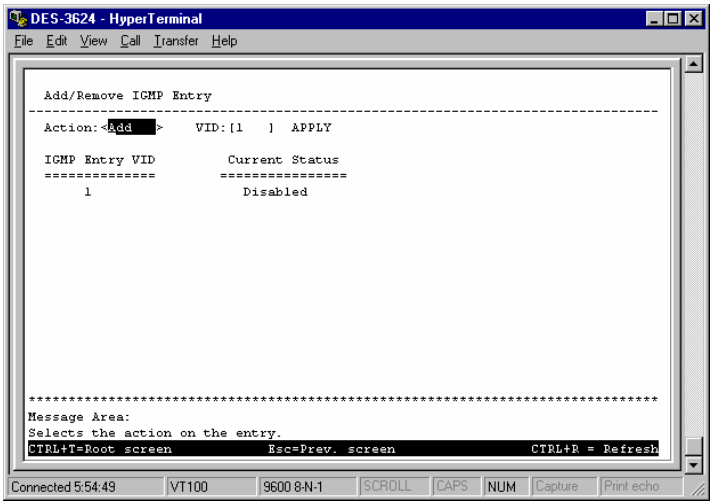


Figure 6-25. Add/Remove IGMP Entry screen

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 12 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 Control Table** in order to activate/deactivate the agents and configure settings for them.

Choose **Configure IGMP Control Table** from the **IEEE 802.1q IGMP Configuration** menu to access the **IEEE 802.1Q IGMP Configuration** screen:

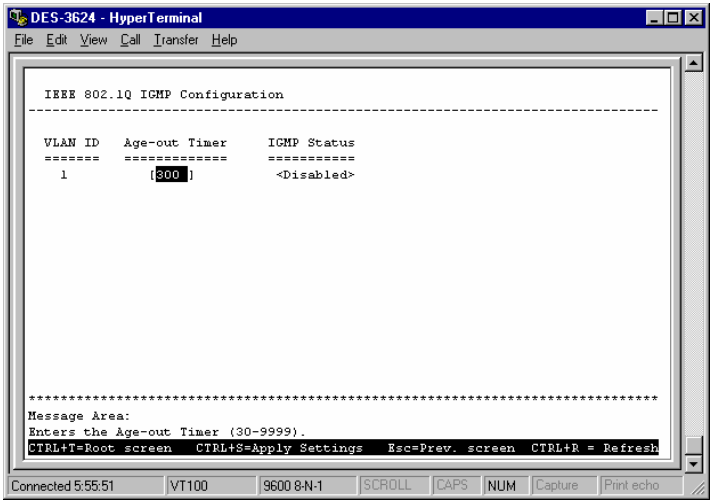


Figure 6-26. IEEE 802.1Q IGMP Configuration screen

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 Timer** If no IGMP query packet has arrived at the Switch before this timer has expired, the Switch will become the IGMP host for this VLAN.

- **IGMP Status** Activates/deactivates the agent on this VLAN.

Configure VLANs & MAC-based Broadcast Domains

The **VLANs & MAC-based Broadcast Domains Configuration** menu displays the status of the current mode and allows a user to restart the Switch in either *IEEE 802.1Q VLANs* (port-based) mode or *MAC-Based Broadcast Domains* mode, or to use neither selection by choosing *NONE*. Please note that the Switch can only support either port-based VLANs or MAC-based broadcast domains at any given time; it cannot support both types simultaneously. You can also access two additional screens, **Configure MAC-based Broadcast Domains** and **Configure IEEE 802.1Q VLANs**.

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

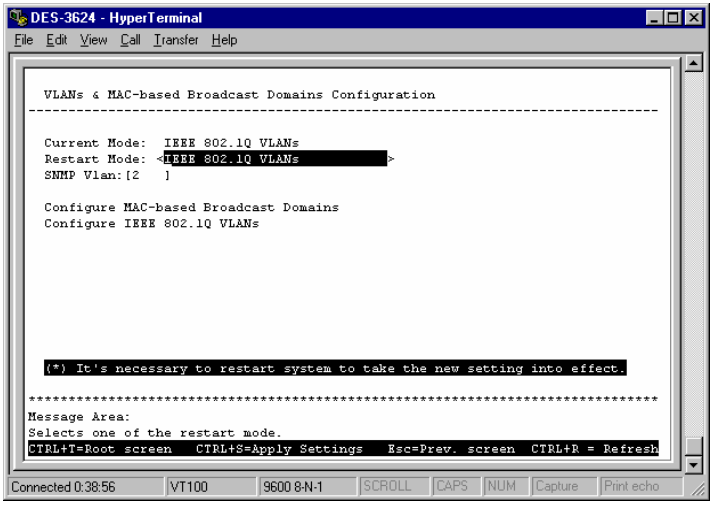


Figure 6-27. VLANs & MAC-based Broadcast Domains Configuration screen

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

- **Current Mode** Displays what mode, if any, is currently enabled on the Switch.

- **Restart Mode** Choose from three settings for this mode: *MAC-Based Broadcast Domains*, *IEEE 802.1Q VLANs*, or *NONE*. After being restarted, the Switch will implement the setting you have chosen.

- **SNMP Vlan** If the *IEEE 802.1Q VLANs* mode is selected, you must also enter a SNMP VLAN ID number in this field. This is a special VLAN that you designate for SNMP management packets. Make sure the Switch port that the management station is connected to has this PVID number and is a static member of this VLAN.

Configure MAC-based Broadcast Domains

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

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

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

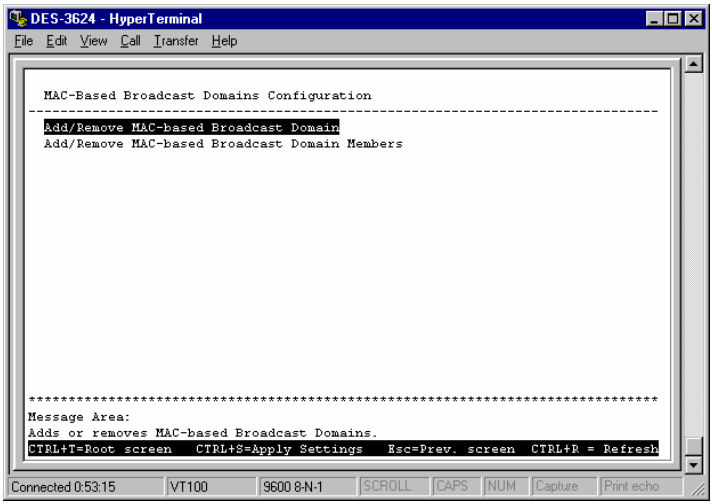


Figure 6-28. MAC-Based Broadcast Domains Configuration menu

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

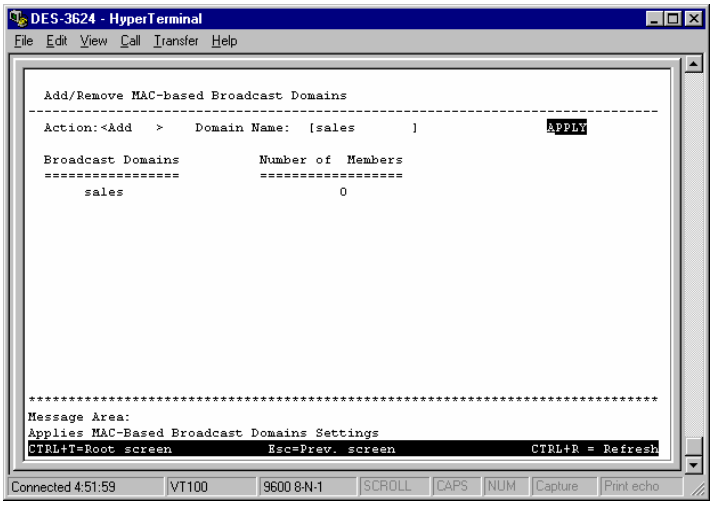


Figure 6-29. Add/Remove MAC-based Broadcast Domains screen

The fields you can set are:

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

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

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

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

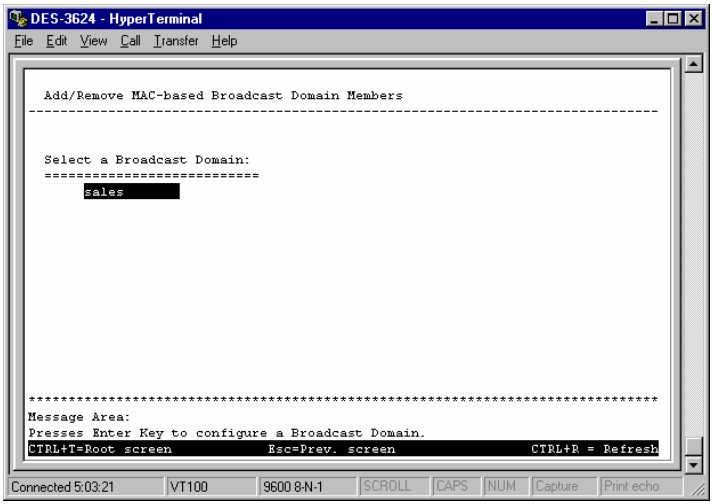


Figure 6-30. Add/Remove MAC-based Broadcast Domain Members screen

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

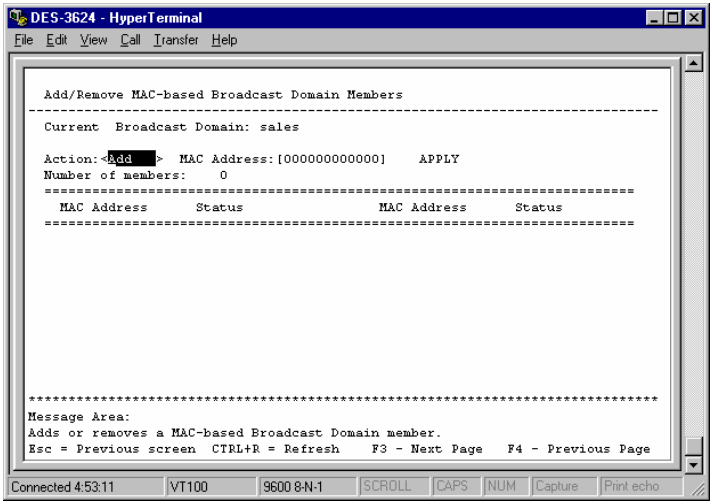


Figure 6-31. Add/Remove MAC-based Broadcast Domain Members screen

The fields you can set are:

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

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

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

Configure IEEE 802.1Q VLANs

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

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

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

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

Choose **Configure IEEE 802.1Q VLANs** on the **VLANs & MAC-based Broadcast Domains Configuration** screen (under **Configure VLANs & MAC-based Broadcast Domains** of the **System Configuration** menu) to access the **IEEE 802.1Q VLANs Configuration** menu:

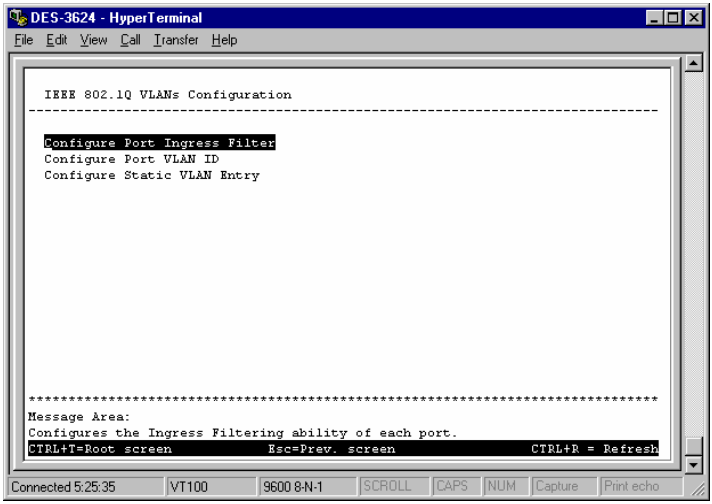


Figure 6-32. IEEE 802.1Q VLANs Configuration menu

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

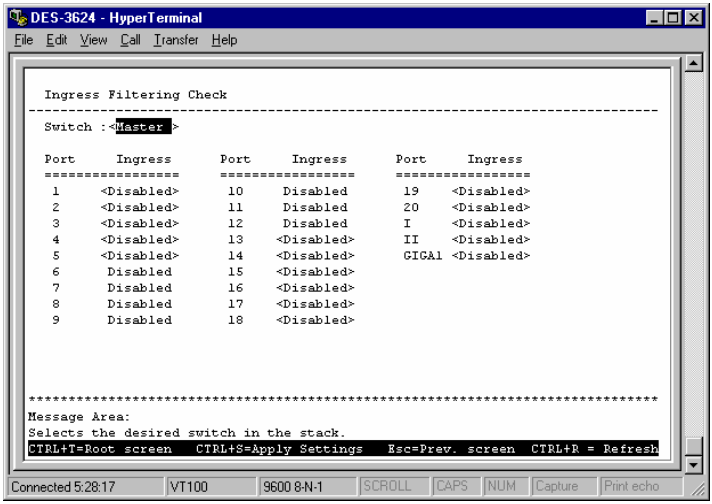


Figure 6-33. Ingress Filtering Check screen

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

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

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

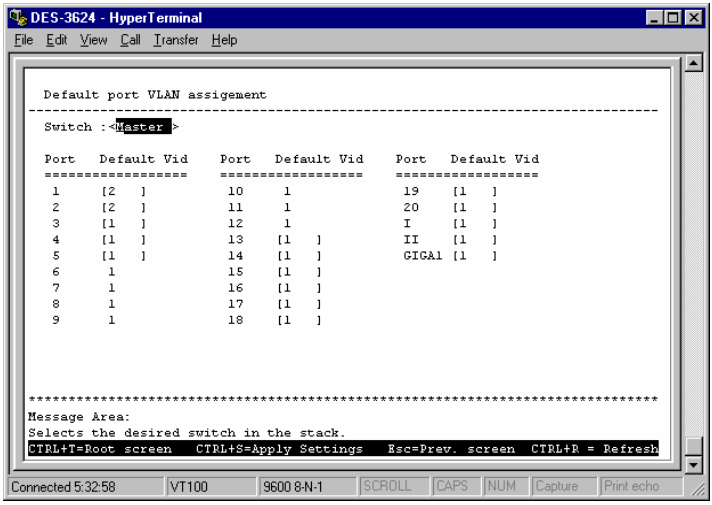


Figure 6-33. Default port VLAN assignment screen

This screen allows you to set a Default port VLAN ID number (Vid) for each port. Press CTRL+S to let the changes take effect.

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

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

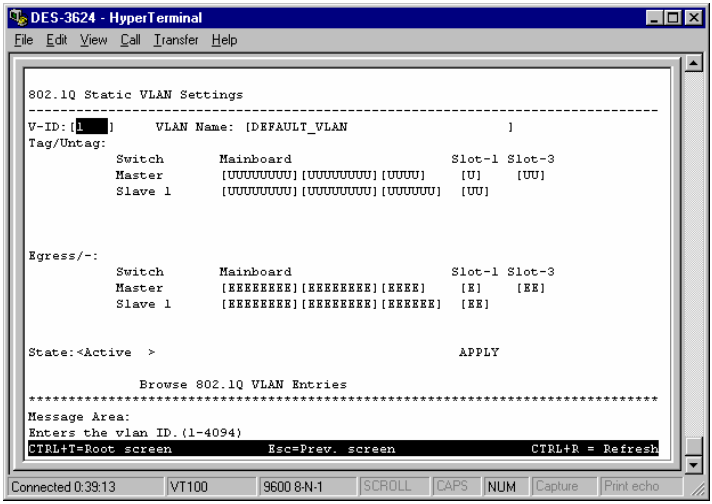


Figure 6-34. 802.1Q Static VLAN Settings screen

The fields you can set are:

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

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

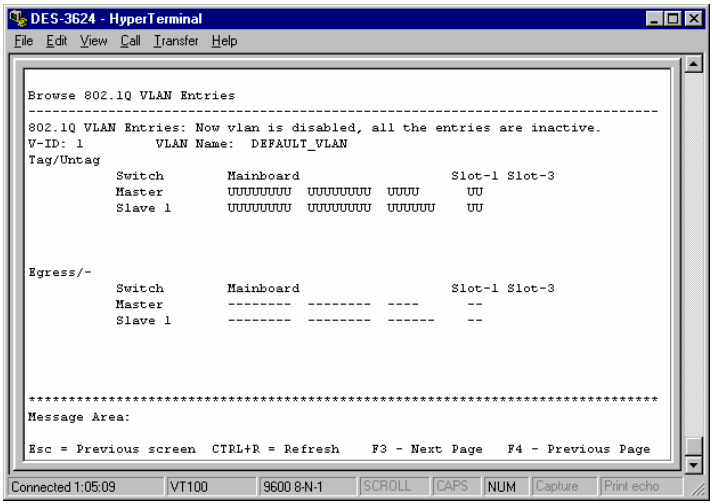


Figure 6-35. Browse 802.1Q VLAN Entries screen

This table displays the *current* **V-ID** and **VLAN Name** as well as **Tag/Untag** and **Egress** (membership) status for all 802.1Q static VLAN entries. Use the F3 key to move to the next page and the F4 key to move to the previous page.

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:

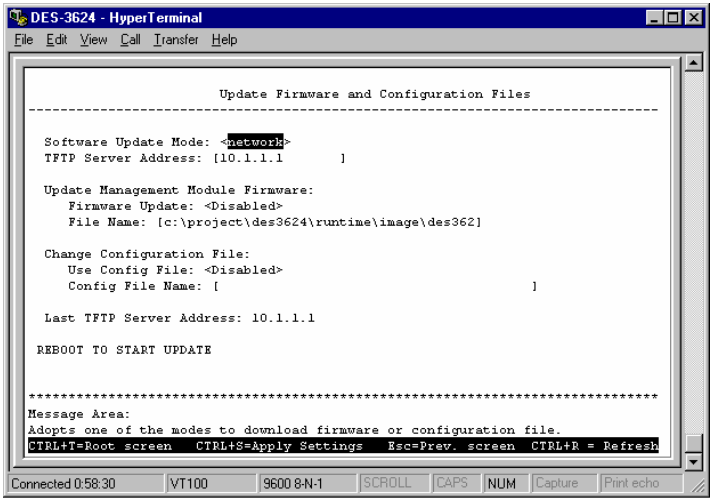


Figure 6-36. Update Firmware and Configuration Files screen

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 through the Ethernet network or through the console port.

- **TFTP Server 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*.

- **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 the settings in a configuration text file when the switch is reset (rebooted). The configuration file is explained in detail in the *Sample Configuration File* Appendix.
- **Config File Name** The complete path and filename on the TFTP server for the configuration file to use.

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

Special Note 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. Firmware updates are handled by the PROM code, which doesn't recognize VLAN tags. You should therefore make sure the Switch port to which the TFTP server is connected is not a tagging port.

System Utilities

The **Utilities** menu offers four system utility options, **Ping Test**, **Save Settings to TFTP Server**, **Save Switch History to TFTP Server**, and **Clear Address Table**.

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

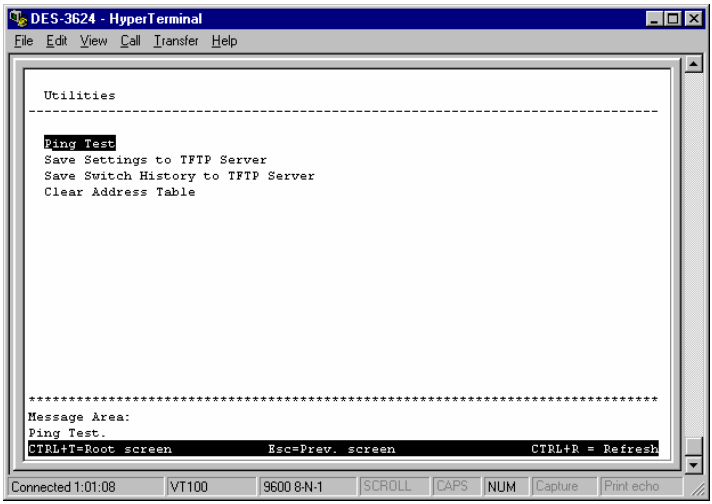


Figure 6-37. Utilities menu

Ping Test

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

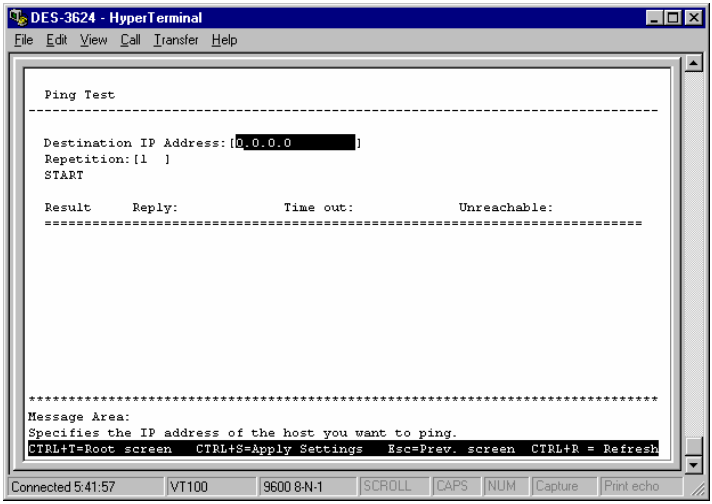


Figure 6-38. Ping Test screen

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.
- **Repetition** Amount of times the Switch should send the Ping (1-255). If zero is chosen, the Switch will continue Pinging indefinitely.

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

Save Settings to TFTP Server

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

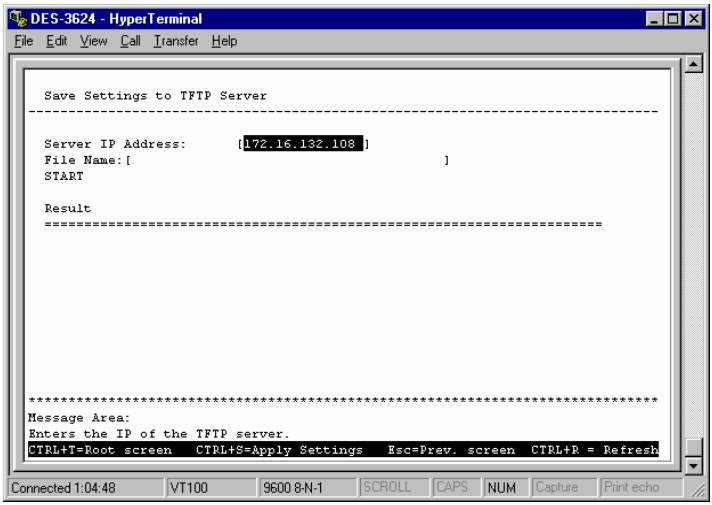


Figure 6-39. Save Settings to TFTP Server screen

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.
- **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:

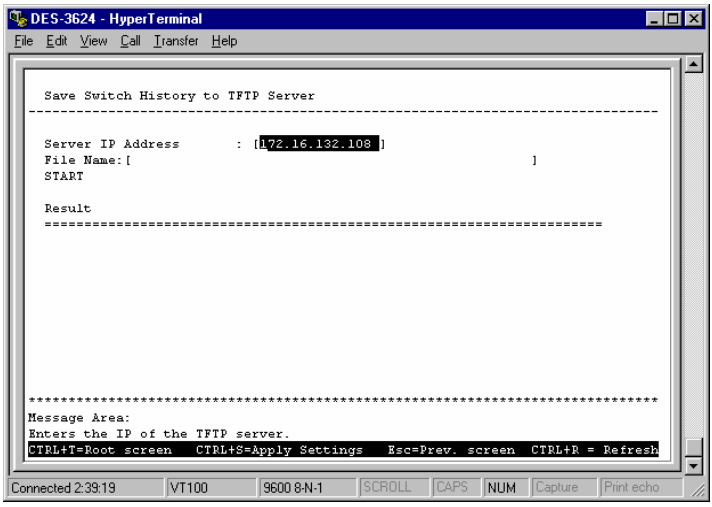


Figure 6-40. Save Switch History to TFTP Server screen

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 the entire Address Table (also known as the Filtering and Forwarding table).

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:

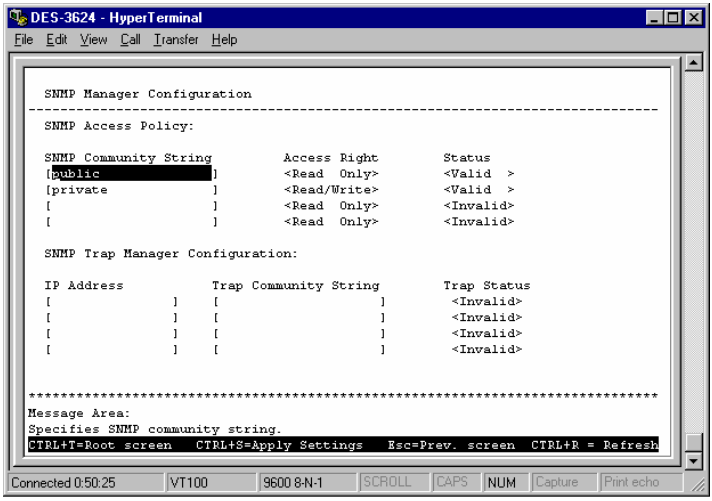


Figure 6-41. SNMP Manager Configuration screen

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

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

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

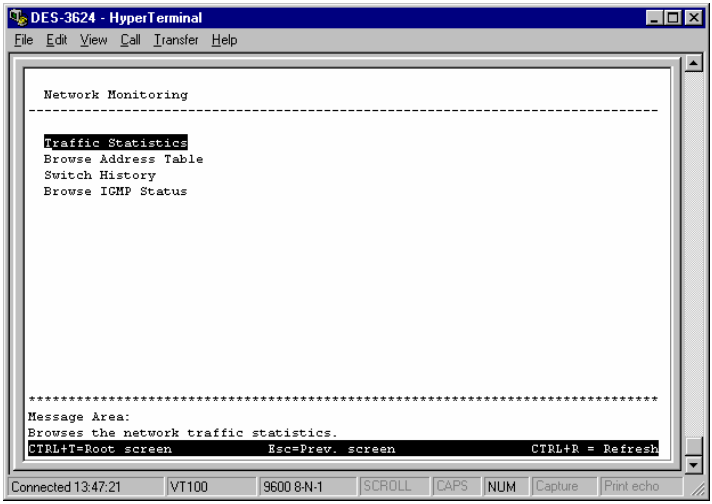


Figure 6-42. Network Monitoring menu

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

Traffic Statistics

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

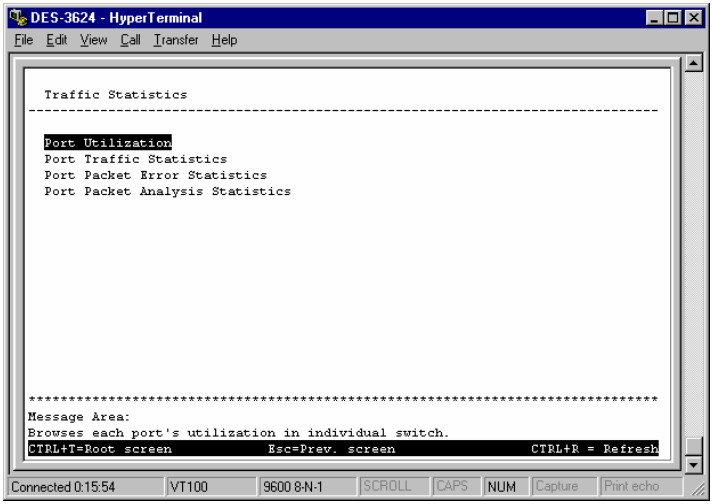


Figure 6-43. Traffic Statistics menu

Port Utilization

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

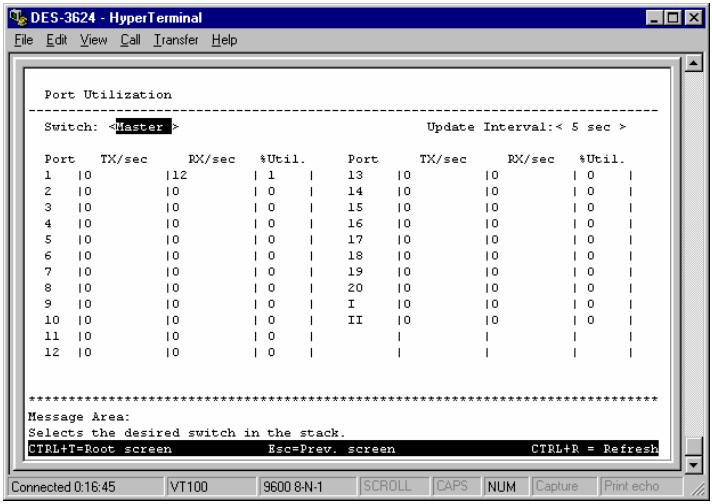


Figure 6-44. Port Utilization screen

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:

- **TX/sec** The number of good bytes sent from the respective port per second.
- **RX/sec** The number of good bytes received per second. This also includes local and dropped packets.
- **%Util.** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval. For example, when a 10 Mbps port is relaying packets at 5 Mbps, the utilization is 50%.

Port Traffic Statistics

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

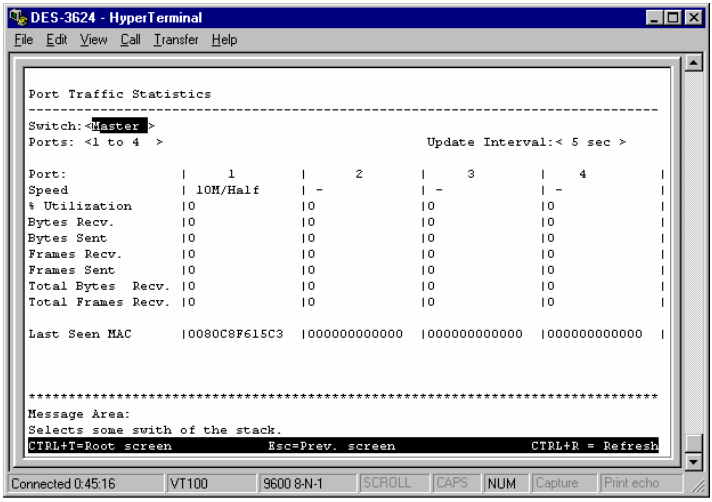


Figure 6-45. Port Traffic Statistics screen

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.

- **% Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval. For example, when a 10 Mbps port is relaying packets at 5 Mbps, the utilization is 50%.

- **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:

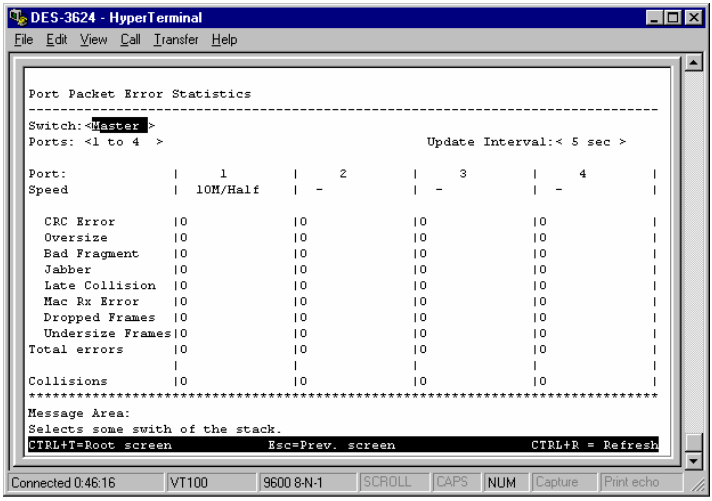


Figure 6-46. Port Packet Error Statistics table

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:

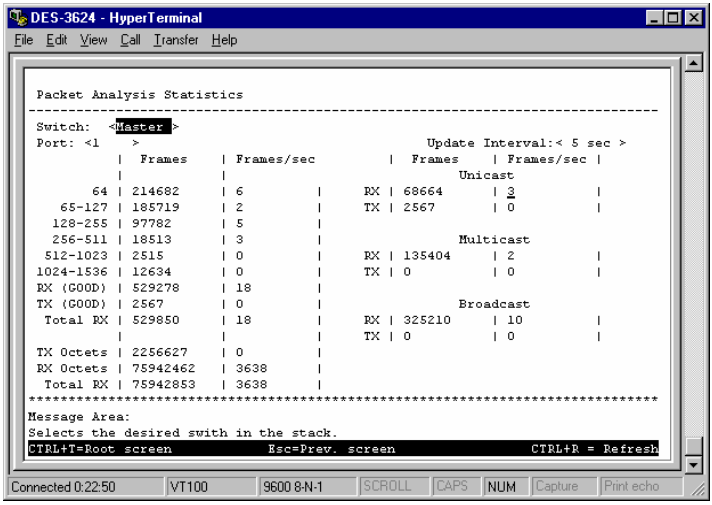


Figure 6-47. Packet Analysis Statistics table

Select the desired device in the **Switch** 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:

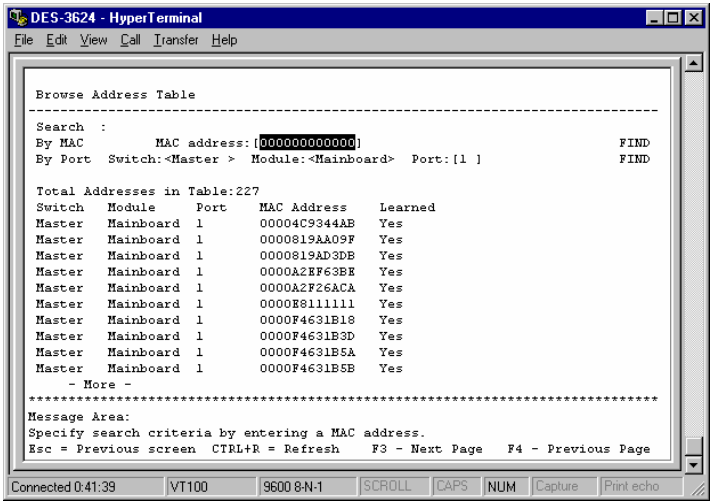


Figure 6-48. Browse Address Table

To browse by MAC address, fill in the **MAC address** field, and then press FIND.

To browse by port number, select the desired **Switch** and **Module** in the respective fields, enter the number of the **Port** you want to configure, and then press FIND.

The lower part of the screen is a read-only Browse Address Table that contains the **Total Addresses in Table**, as well as the **Switch**, **Module**, **Port**, **MAC Address**, and **Learned** status of each entry. Use F3 to advance to the next page and F4 to return to the previous page.

Switch History

The **Network Monitoring** 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 is 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:

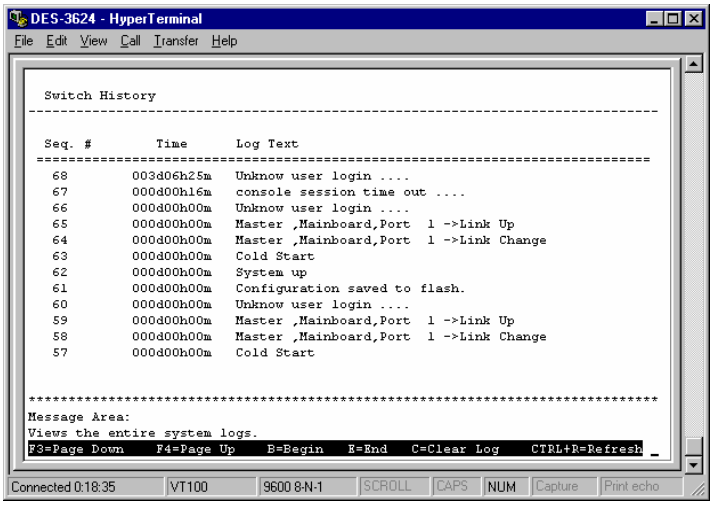


Figure 6-49. Switch History screen

The switch history entries are listed chronologically from the last time the Switch was rebooted. Use the following keys to move around the screen above: F3 – Page down, F4 – Page up, B – Begin, E – End, and C – Clear Log. CTRL+R will refresh the screen.

Browse IGMP Status

The **Browse IGMP Status** function allows you to browse Internet Group Management Protocol (IGMP). The Switch is able to recognize IGMP queries and reports sent between

stations and an IGMP router. When enabled for IGMP snooping, the Switch can open or close a port to specific devices based on the IGMP messages sent from the device to the router or vice versa.

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

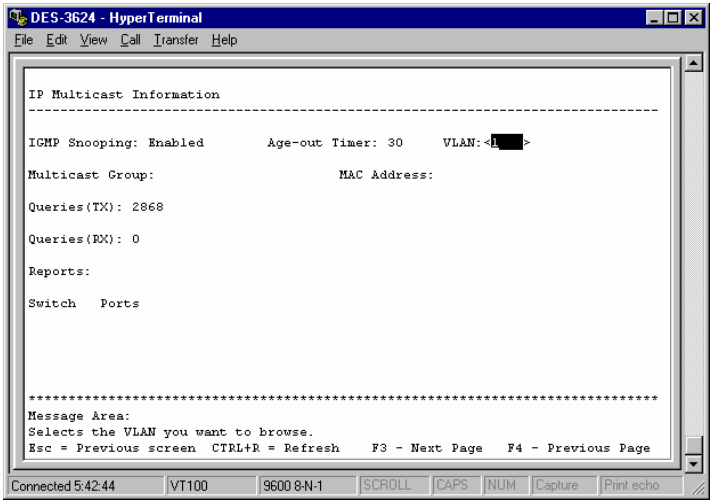


Figure 6-50. IP Multicast Information screen

This screen displays the number of IGMP queries and reports for each active IP multicast group detected by the Switch. You can also view which Switch ports support each multicast group and enter a VLAN number in the field on the right.

The fields displayed are defined as follows:

- **IGMP Snooping** Indicates whether IGMP snooping is *Enabled* or *Disabled*.

- **Age-out Timer** Displays the time the Switch waits between IGMP queries.
- **VLAN** Enter the desired VLAN ID number.
- **Multicast Group** The Multicast IP address of the Multicast group being displayed.
- **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

You can use the console interface to reset the Switch, either performing a **Restart System** or a **Factory Reset** (which sets all of the Switch's parameters to what they were when the Switch was delivered from the factory).

Restart System

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

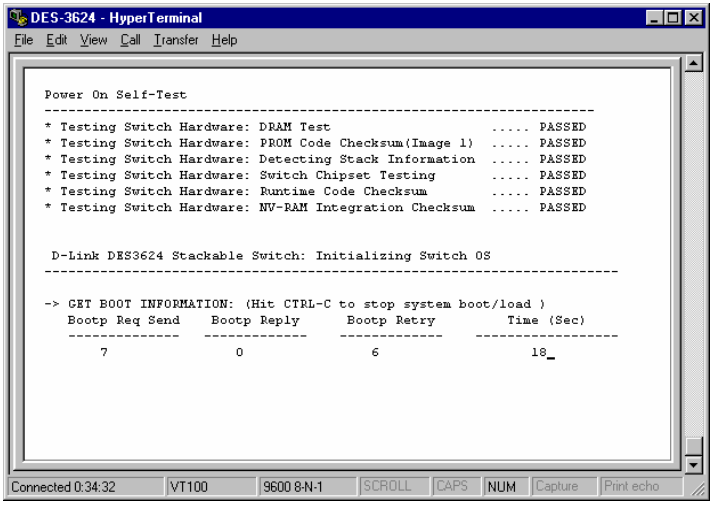


Figure 6-51. Restart System screen

Factory Reset

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

Note: 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:

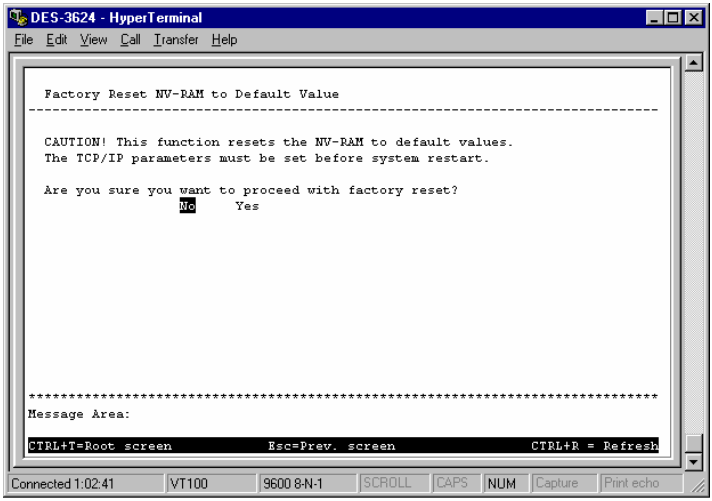


Figure 6-52. Factory Reset NV-RAM to Default Value screen

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, 4.x or later, or Microsoft Internet Explorer, 4.x 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 two bytes per character).

Getting Started

The first step in getting started in using Web-based management for your Switch is to secure a browser. A Web browser is a program that allows a person to read hypertext, for example, Netscape Navigator, 4.x or later, or Microsoft Internet Explorer, 4.x or later. 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-3624 Manager** button:

This opens the main page in the management module.

The top of each page contains an interactive view of the Switch's front panel. If your Switch is part of a stack, there will also be an icon representing each Switch in the stack on the

left side of this panel. Click on the desired Switch to view that Switch's front panel. A colored border around the Switch icon

indicates which Switch's front panel is currently being displayed:

Clicking on one of the ports 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. Clicking on one of the categories causes a list of options to appear below.

The switch management features are explained below.

Configuration

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

IP Address

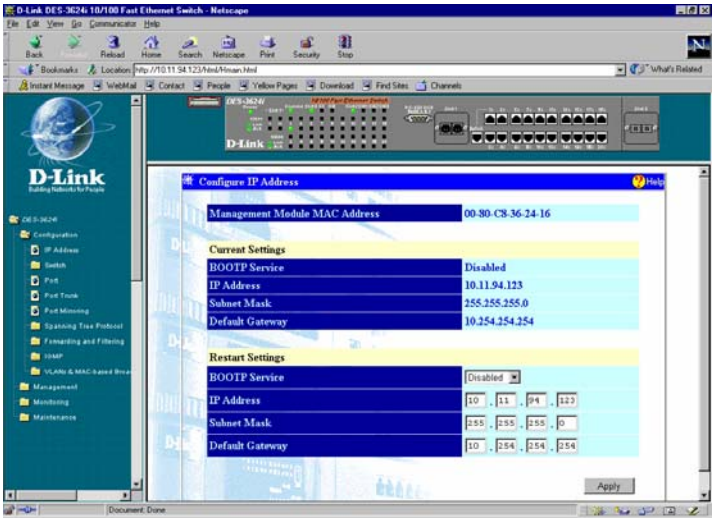


Figure 7-1. Configure IP Address window

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:

- **Management Module MAC Address** The Ethernet address for the device. Also known as the physical address.

- **BOOTP Service** The BOOTP protocol allows IP addresses, subnet masks, and default gateways to be assigned on a central BOOTP server. If this option is

enabled, when the Switch is first powered up it will look for a BOOTP server to provide it with this information before using the supplied settings.

- **IP Address** The host address for the device 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

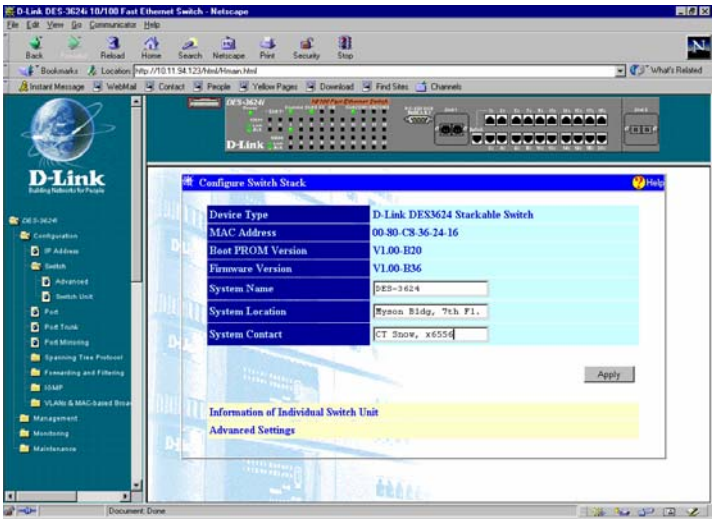


Figure 7-2. Configure Switch Stack window

To set basic Switch settings, enter a **System Name** in the first field, the physical location of the Switch in the **System**

Location field, and the name of the contact person responsible for the Switch in the **System Contact** field. Then click **Apply**.

Two hyperlinks at the bottom of this window provide access to the **Information Of Individual Switch Unit** and **Configure Switch Stack – Advanced** windows, respectively. These windows are described in the two sections that immediately follow.

The information in the window above is described as follows:

- **Device Type** A description of the Switch type.
- **MAC Address** The Ethernet address for the device.
- **Boot PROM Version** Version number for the PROM code.
- **Firmware Version** Version number of the firmware installed on the Switch. This can be updated by using the **Firmware and Configuration Update** window in the Maintenance section.
- **System Name** A user-assigned name for the Switch.
- **System Location** A user-assigned description of the physical location of the Switch.
- **System Contact** Name of the person to contact should there be any problems or questions with the system. You may also want to add a phone number or extension.

Advanced

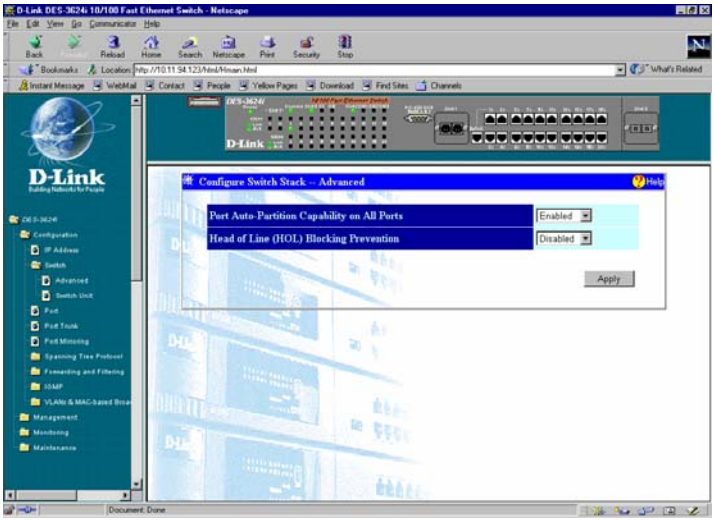


Figure 7-3. Configure Switch Stack – Advanced window

The first setting allows you to enable or disable port auto-partitioning by the **Port's 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, which is designed to prevent forwarding a packet to a "blocking" port. Click **Apply** to let your changes take effect.

The information above is described as follows:

- **Port's Auto-Partition Capability on All Ports** This option offers *Enabled* or *Disabled* to decide whether to auto-partition a selected port and take it offline or not.

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

Switch Unit

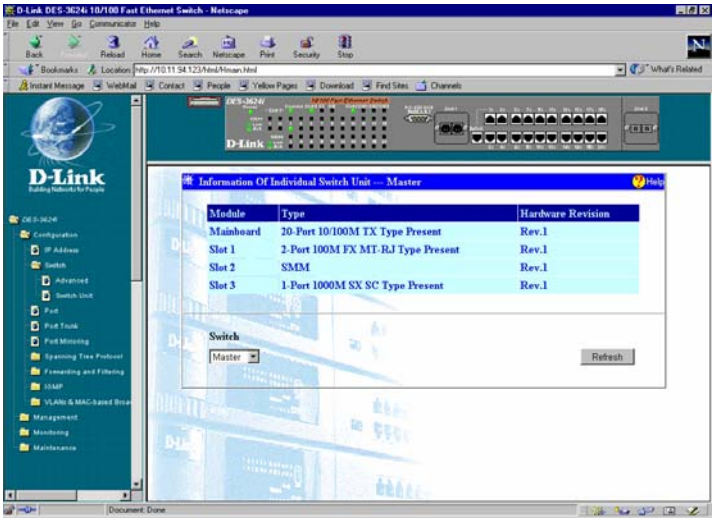


Figure 7-4. Information Of Individual Switch Unit window

This window displays the **Module**, **Type**, and **Hardware Revision** of each individual Switch unit. Select the desired Switch in the field in the lower left-hand corner. A **Refresh** button is located in the lower right-hand corner.

The information above is described as follows:

- **Module** The module location in the Switch unit.
- **Type** The type of module in the Switch unit.
- **Hardware Revision** Version number of the module's hardware in the Switch unit.

Port

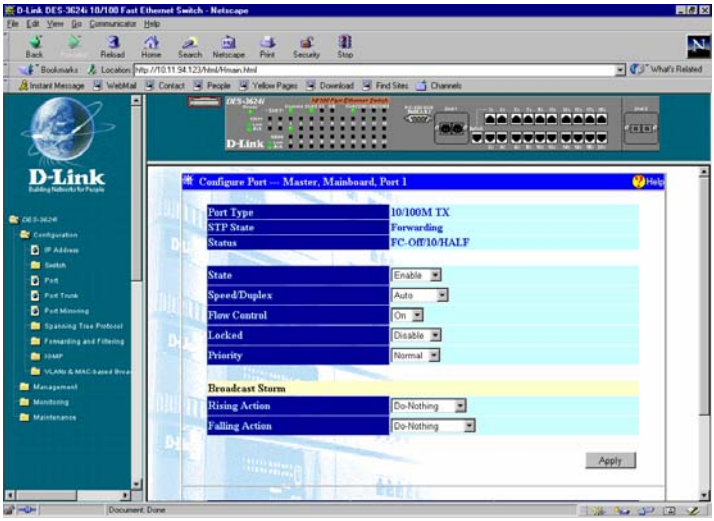


Figure 7-5. Configure Port window

Select the port you want to configure by clicking on the port in the Switch front panel display at the top of the screen or by using the **Switch**, **Slot**, and **Port** fields at the bottom of the screen. Then follow these steps:

1. Enable or disable the port in the **State** field. 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 **Static 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.

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* (NWay) in the speed/duplex field above and flow control is enabled, flow control (whether full- or half-duplex) will only be implemented if the other device can auto-negotiate flow control. Note that you must reboot the Switch before a flow control change can take effect.

4. 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 *Enabled* or *Disabled*.

5. Configure the **Priority** setting for packets passing through this port, using IEEE 802.1p/q tagging. Select *Low*, *High* or *Default*. If the network is congested, the

Switch handles packets with a higher priority before those with lower priority.

6. Configure the **Rising Action** setting under **Broadcast Storm** from three choices: *Do Nothing*, *Blocking*, or *Blocking-Trap*.

7. Configure the **Falling Action** setting under **Broadcast Storm** from three choices: *Do Nothing*, *Forwarding*, or *Forwarding-Trap*.

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.

Port Trunk

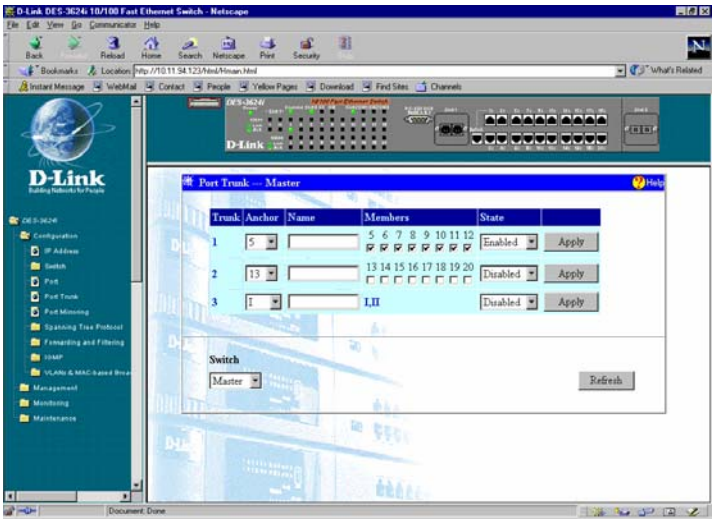


Figure 7-6. Port Trunk window

The Switch supports up to three 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*.
- **Switch** This field allows you to select the desired Switch.

Port Mirroring

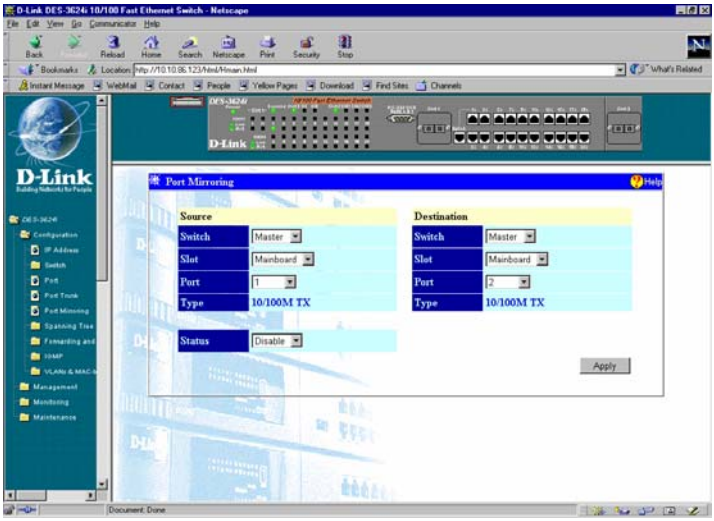


Figure 7-7. Port Mirroring window

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 **Switch**, **Slot**, and source **Port** from where you want to copy frames in the Source section. Next, select the **Switch**, **Slot** and target **Port** which will receive the copies from the source port in the Destination section. This is the port 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 from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group.

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 Parameters Setting

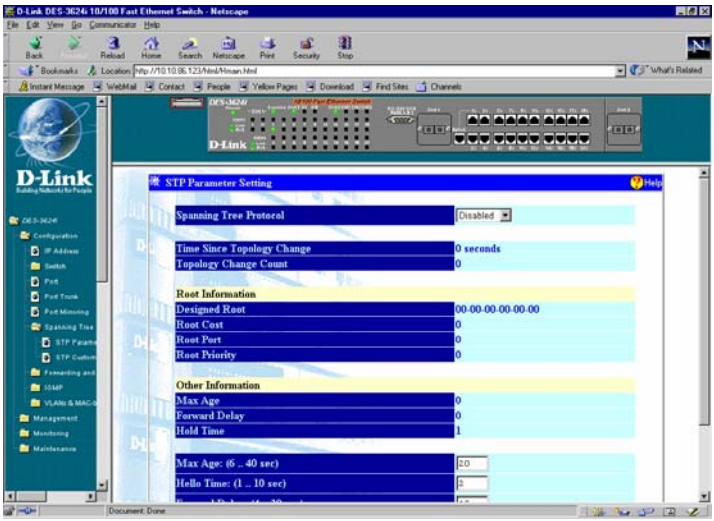


Figure 7-8. STP Parameter Setting window

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

The information above is described as follows:

- **Spanning Tree Protocol** This option offers *Disabled* or *Enabled* to implement the Spanning Tree Protocol.
- **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 Custom Setting

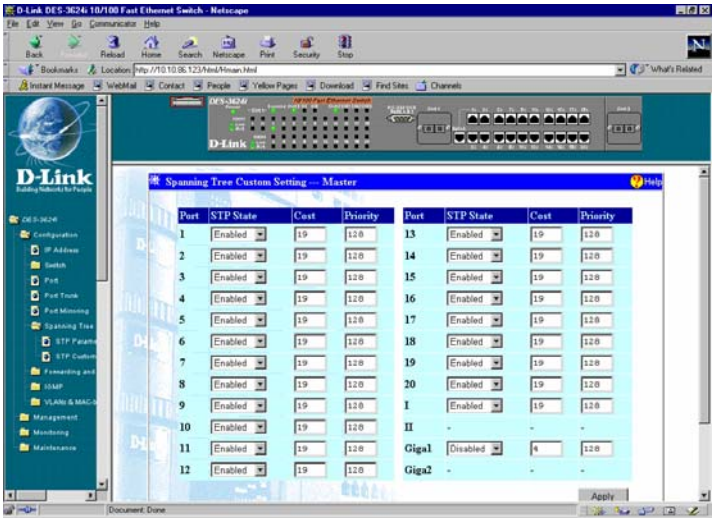


Figure 7-9. Spanning Tree Custom Setting window

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

The information above is described as follows:

- **STP State** The Spanning Tree Protocol state for a selected port can either be *Enabled* or *Disabled*.
- **Cost** The Path Cost is a changeable parameter and may be modified according to the Spanning Tree Algorithm specification. Each 10 Mbps and 100Mbps segment has an assigned Path Cost of 19.
- **Priority** Priority is a read-write object that can be set from 0 to 255. This is the priority number of the port. The lower the port priority, the more chance the bridge

has of becoming the root 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.

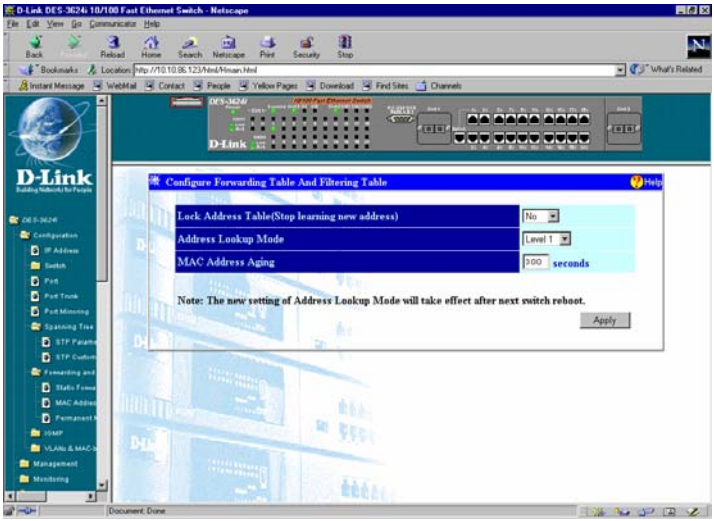


Figure 7-10. Configure Forwarding Table And Filtering Table window

This window allows you to stop or start address learning, use an address look-up mode, and select an age-out time of the MAC address in the selected address table. Click **Apply** to let your changes take effect.

The following fields above can be set:

- **Lock Address Table(Stop Learning)** 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 coming from an unknown source address will be dropped by the Switch.

- **Address Look-up Mode** Select from: *Level 0*, *Level 1*, *Level 2*, *Level 3*, *Level 4*, *Level 5*, *Level 6*, or *Level 7*.

- **MAC Address Age-out Time (sec.)** Enter the desired MAC address aging time in this field (10 to 9999 seconds).

Static Forwarding Table

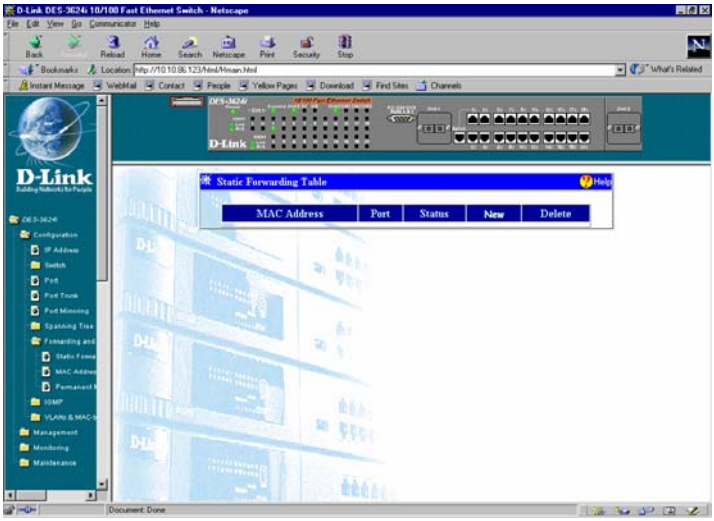


Figure 7-11. Static Forwarding Table window

MAC forwarding allows the Switch to permanently forward outbound traffic to specific destination MAC addresses over a

specified port. You can also use this feature to restrict inbound traffic based on source MAC addresses.

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

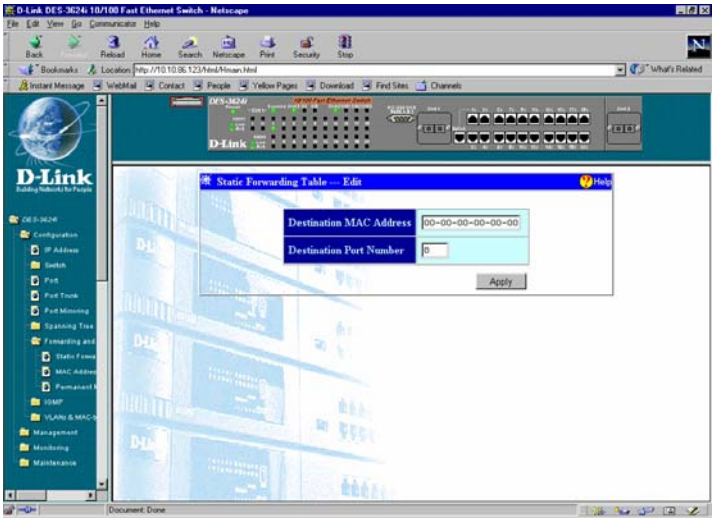


Figure 7-12. Static Forwarding Table---Edit window

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

The information above is described as follows:

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

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

MAC Address Filtering Table

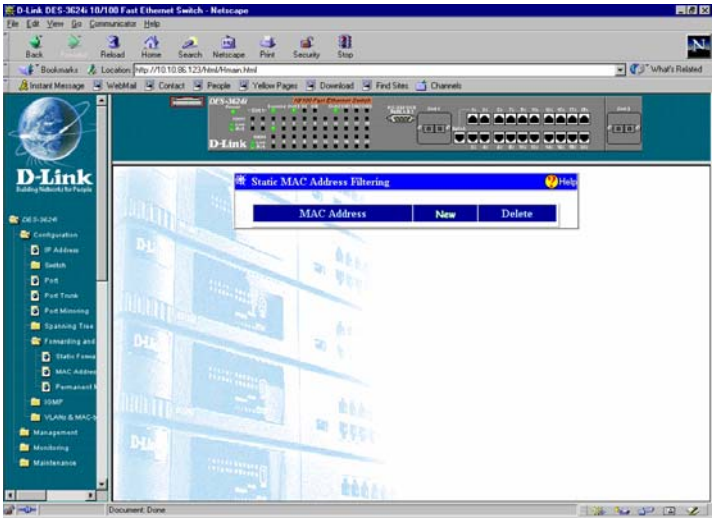


Figure 7-13. Static MAC Address Filtering window

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

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

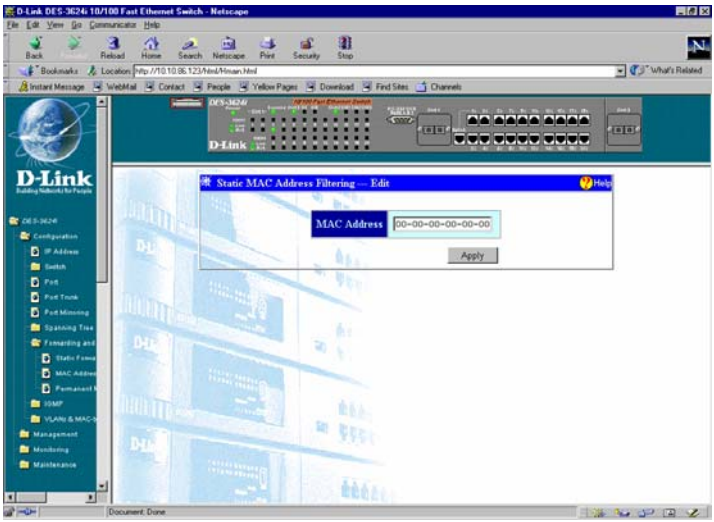


Figure 7-14. Static MAC Address Filtering---Edit window

To use the static filtering function, enter the MAC address of the device allowed to send traffic in the **MAC Address** field and then click **Apply**.

The information above is described as follows:

- **MAC Address** The Ethernet address of the Static MAC Address Filtering table entry.

Permanent Multicast Filtering

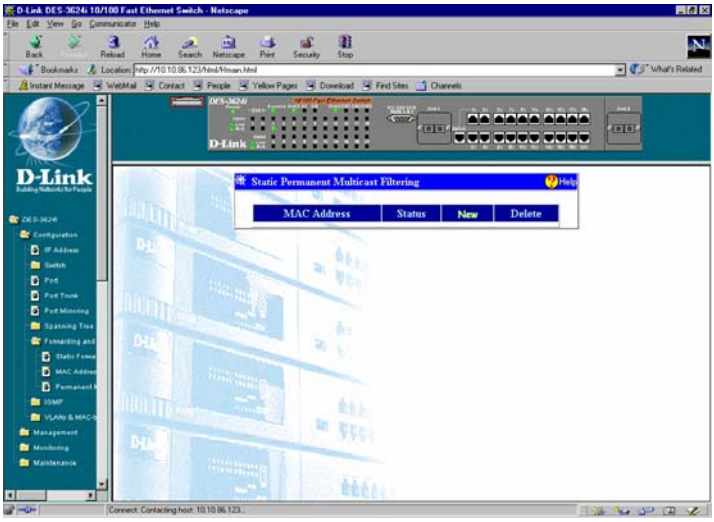


Figure 7-15. Static Permanent Multicast Filtering window

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.

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

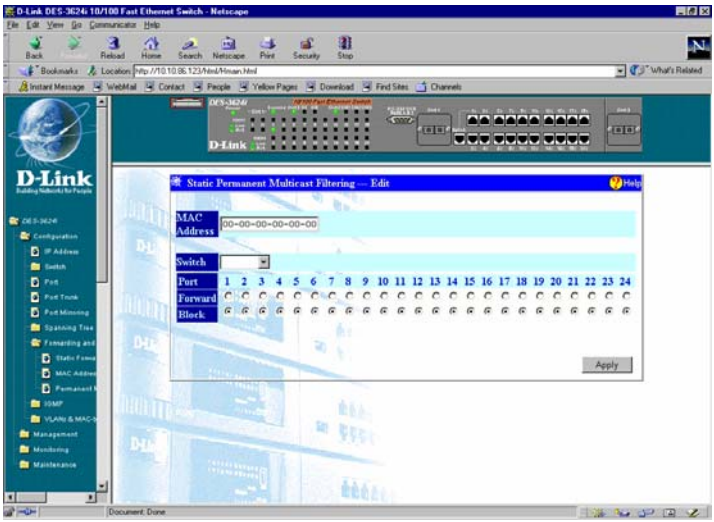


Figure 7-16. Static Permanent Multicast Filtering--Edit window

To edit or create a new filter, enter the MAC address in the **MAC Address** field, select the desired **Switch** and **Port** in the next two fields. Next, select **Forward** or **Block** for each port, deciding whether that port transmits or blocks traffic for the specified multicast group. Click **Apply** to activate the filter.

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

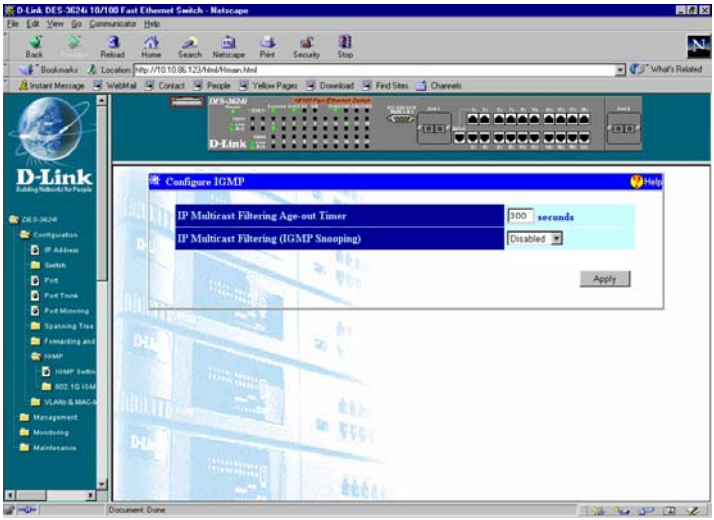


Figure 7-17. Configure IGMP window

To configure the IGMP, enter a value between 30 and 999 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

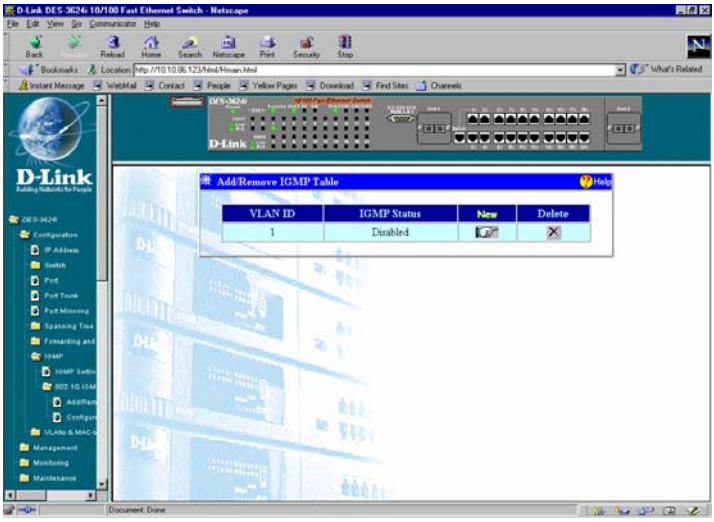


Figure 7-18. Add/Remove IGMP Table window

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

Click the pointer icon on the far right to access the **Add/Remove IGMP Table-Edit** window:

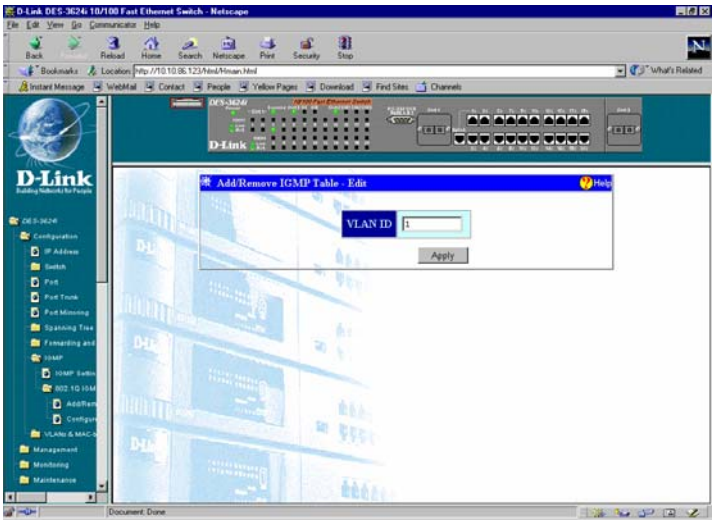


Figure 7-19. Add/Remove IGMP Table-Edit window

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

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.

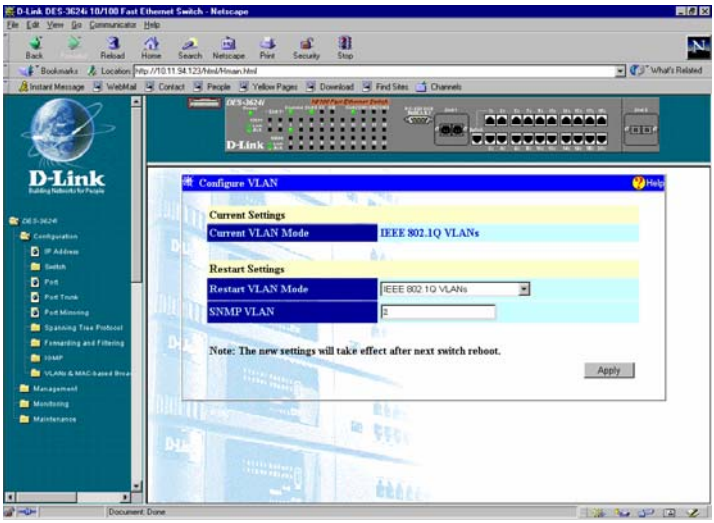


Figure 7-20. Configure VLAN window

To use one of these two modes, select *MAC-based Broadcast Domains* or *IEEE 802.1Q VLANs* under **Restart VLAN Mode**--otherwise, leave the setting at *Disabled*. Then specify the VLAN ID number in the **SNMP VLAN** field and click **Apply**. The SNMP VLAN ID sets up a VLAN for management packets.

MAC-Based Broadcast Domains

To use MAC-based Broadcast Domains, you must first create a MAC-based Broadcast Domain using the add/remove function and then add members to the Broadcast Domain using the add/remove member function.

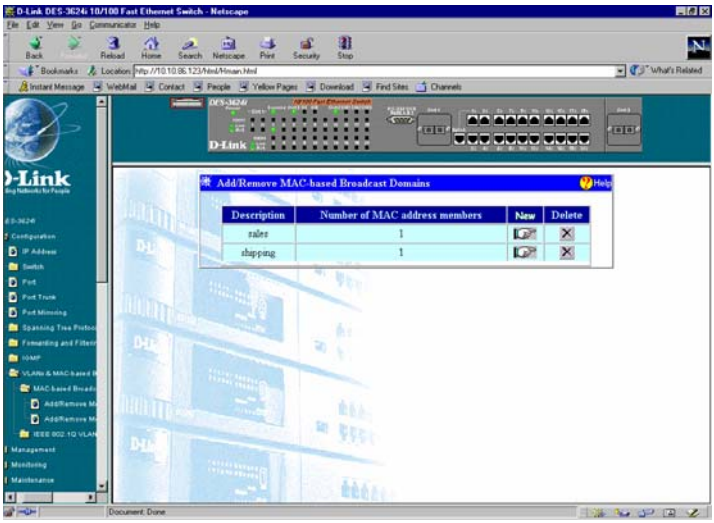


Figure 7-21. Add/Remove MAC-based Broadcast Domains window

Items in this window are defined as follows:

- **Description** Lists all MAC-based broadcast domains.
- **Number of MAC address members** The number of MAC addresses belonging to the Broadcast Domains.

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

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

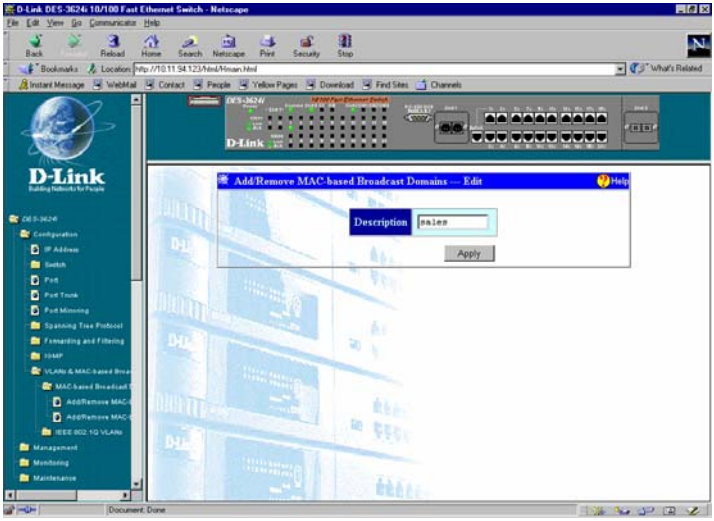


Figure 7-22. Add/Remove MAC-based Broadcast Domains --- Edit window

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 Broadcast Domain to be added.

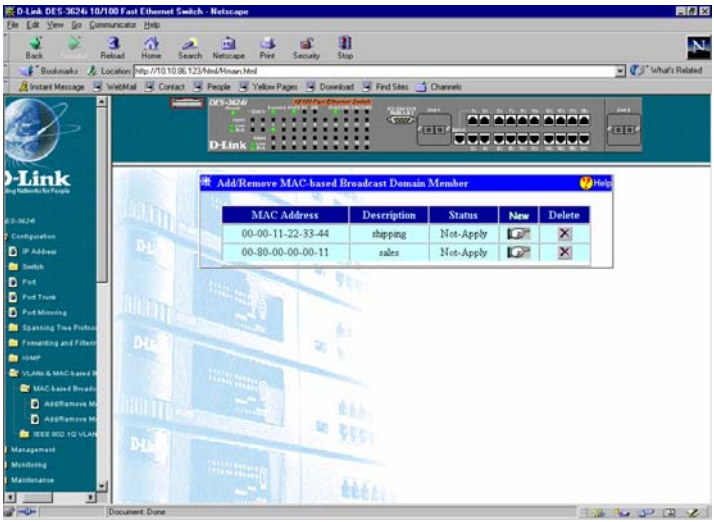


Figure 7-23. Add/Remove MAC-based Broadcast Domain Member window

Items in this window are defined as follows:

- **MAC Address** The MAC Address of the broadcast domain member.
- **Description** Lists all MAC-based broadcast domains.
- **Status** *Not-Apply* or *Apply* will be displayed here

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

Click **New** to access the **Add/Remove MAC-based Broadcast Domain Member --- Edit** window:

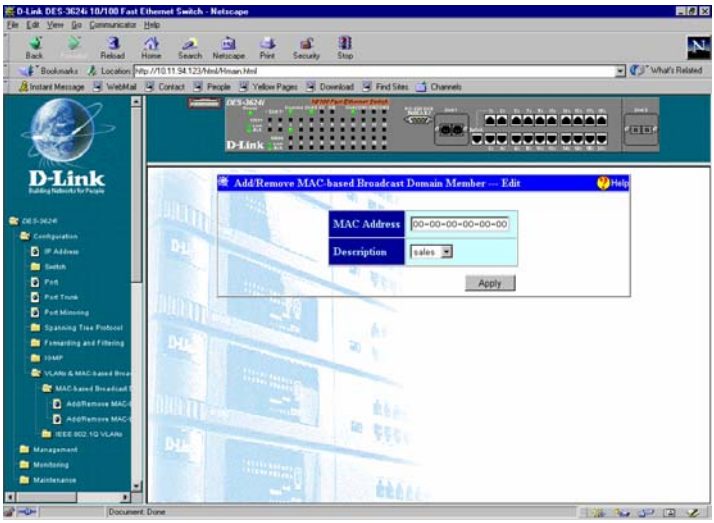


Figure 7-24. Add/Remove MAC-based Broadcast Domain Member --Edit window

To add or edit a MAC-based broadcast domain member, enter the **MAC Address** in the first field and use the drop-down **Description** menu to select the desired broadcast domain. Click **Apply** to let the changes take effect.

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.

IEEE 802.1Q VLANs

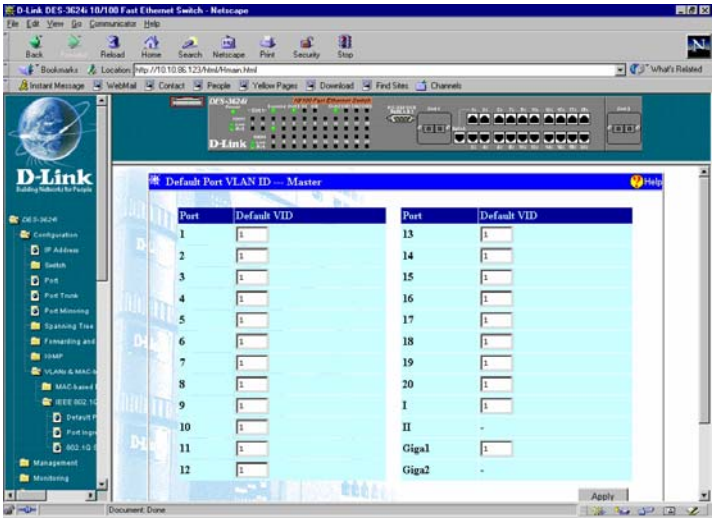


Figure 7-25. Default Port VLAN ID window

Use this window to assign a default VLAN ID for each desired port. Click **Apply** to let the settings take effect.

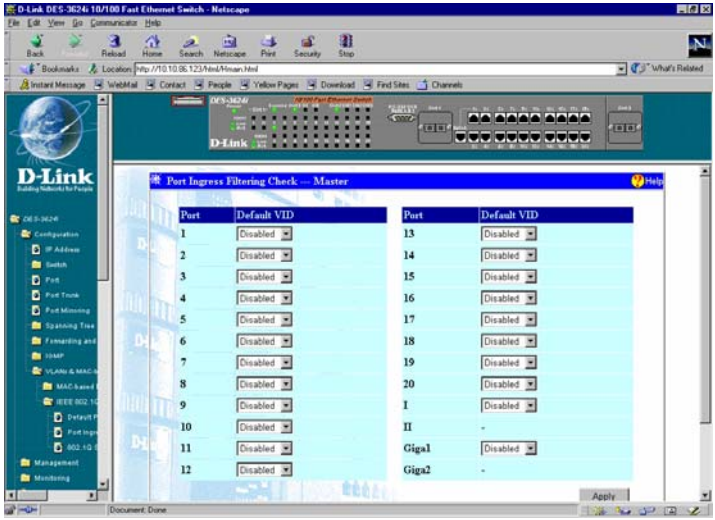


Figure 7-26. Port Ingress Filtering Check window

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

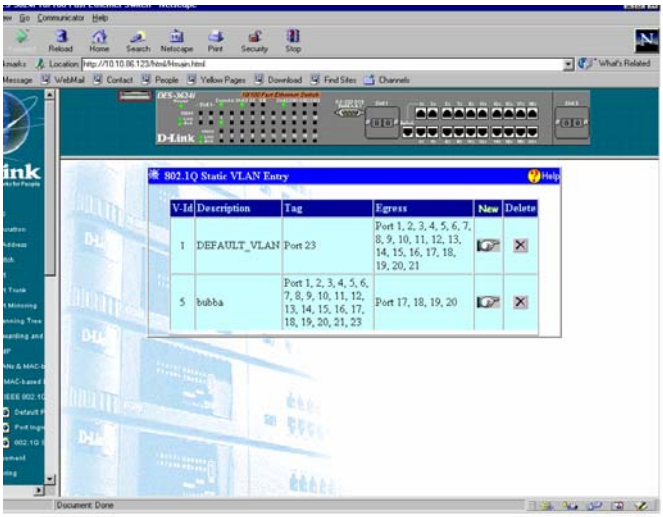


Figure 7-27. 802.1Q Static VLAN Entry window (number one)

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

Click the pointer icon to access the second **802.1Q VLAN Entry** screen:

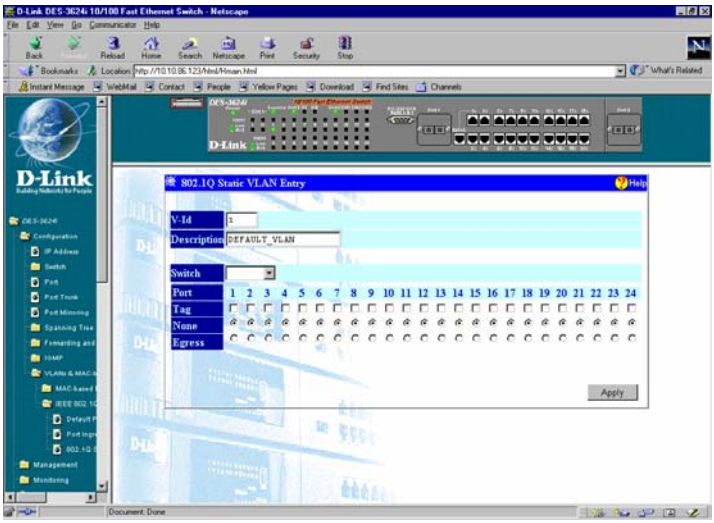


Figure 7-28. 802.1Q Static VLAN Entry window (number two)

To configure an 802.1Q VLAN entry, enter a **V-Id** number and **Description** in the first two fields. Next, select the desired **Switch**. 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 belong to a VLAN. Otherwise, check **Egress** to statically set a port to belong to a VLAN. Click **Apply** to let the changes take effect.

Management

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

Community Strings and Trap Stations

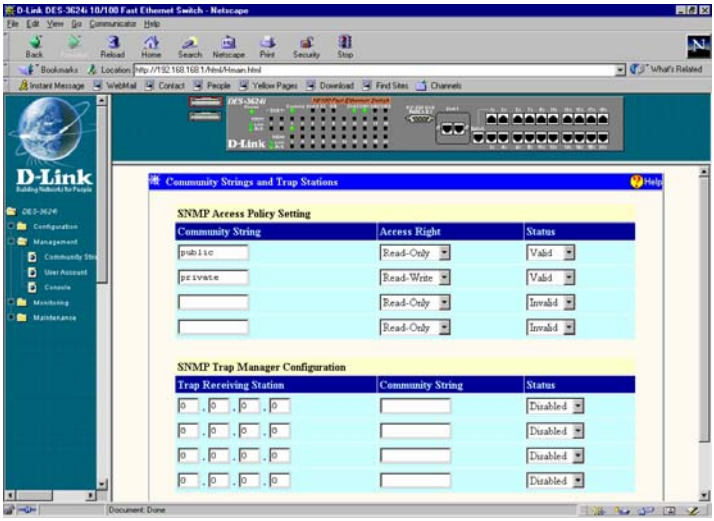


Figure 7-29. Community Strings and Trap Stations window

To use the functions on this window, enter the appropriate SNMP information in the Community Strings and Trap Receiving Stations 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 information is described as follows:

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

- **Status** Option to set the current community string to *Valid* or *Invalid*.

The SNMP Trap Manager Configuration information is described as follows:

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

User Account

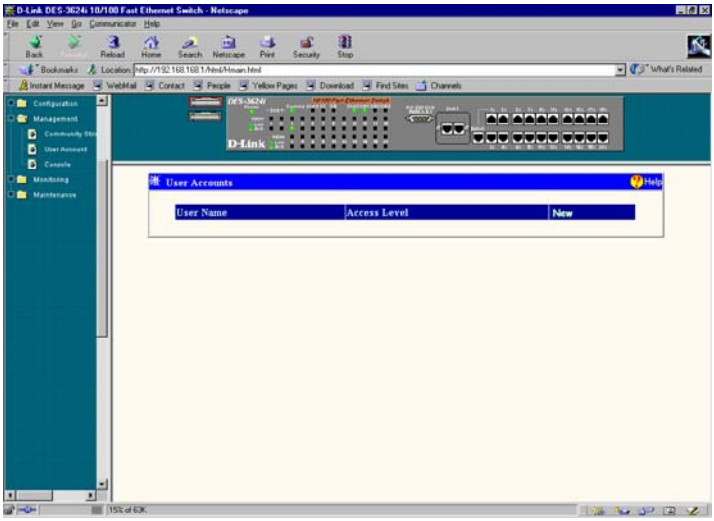


Figure 7-30. User Accounts window

Click the pointer icon on the right-hand side to access the **User Account - Edit** window:

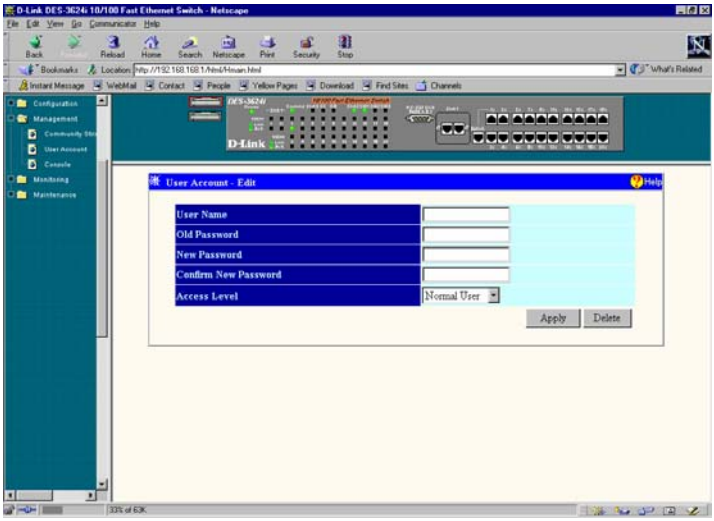


Figure 7-31. User Account-Edit window

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

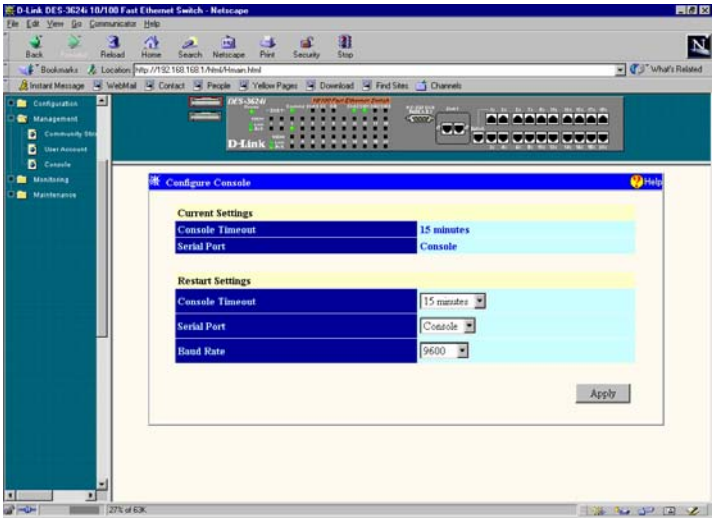


Figure 7-32. Configure Console window

This window allows you to choose the refresh rate in the **Console Timeout** field (*15 minutes*, *30 minutes*, *45 minutes*, *60 minutes* or *Never*). Select the protocol for communicating through the console port, *Console* or *SLIP,* in the **Serial Port** field. Use SLIP for out-of-band management. If SLIP is being used, you may also set the **Baud Rate** in the last field. Click **Apply** and then reboot the Switch for console port settings to take effect.

The default serial port settings are:

- Baud Rate=9600
- Data Bits=8
- Flow Control=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 Statistics**, **Browse Address Table**, **Browse IGMP Status**, and **Switch History**.

Switch Overview

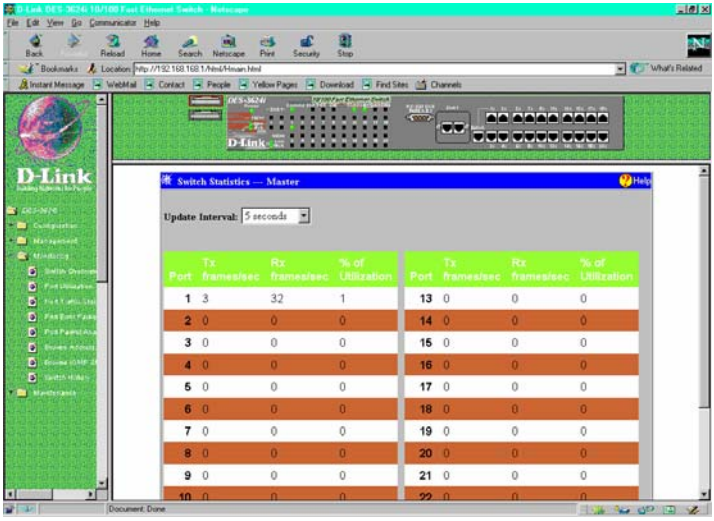


Figure 7-33. Switch Statistics window

The information is described as follows:

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

- **Port** The selected port to be monitored.

- **TX frames/sec** Counts the total number of frames transmitted from a selected port per second since the Switch was last rebooted.

- **RX frames/sec** Counts all valid frames received on the port per second since the Switch was last rebooted.

- **% of Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval. For example, when a 10 Mbps port is relaying packets at 5 Mbps, the utilization is 50%.

Port Utilization

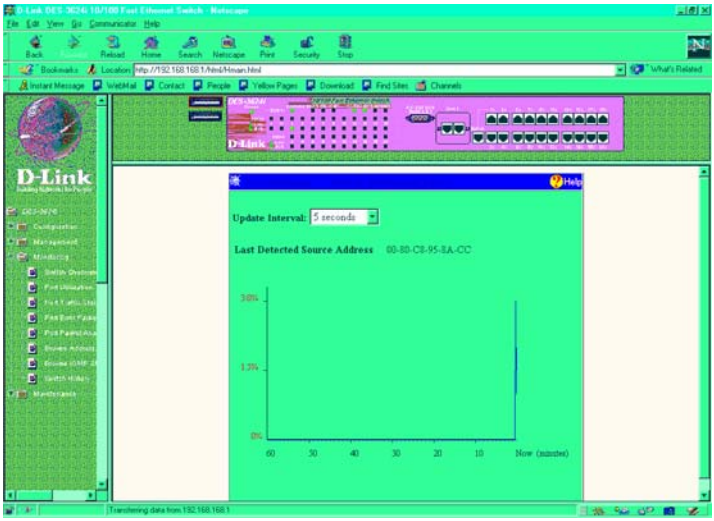


Figure 7-34. Port Utilization window

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

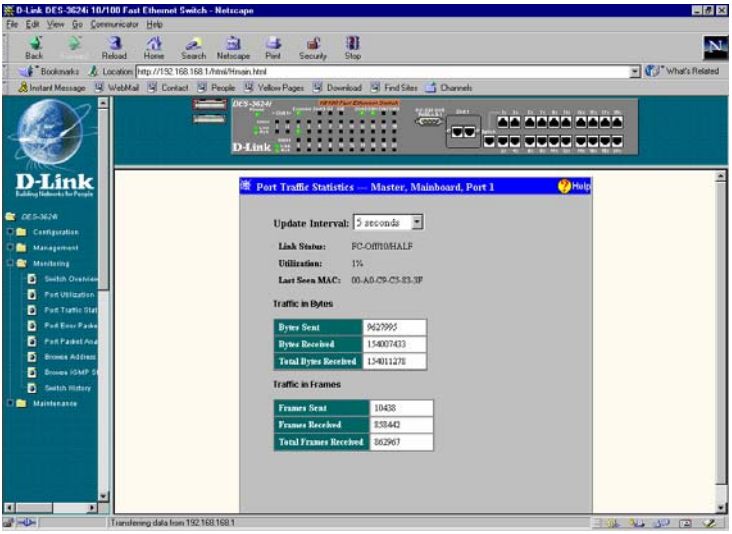


Figure 7-35. Port Traffic Statistics window

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 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*.
- **Link Status** Indicates whether the port is online and working (*On*) or not (*Off*).
- **Utilization** Current utilization for the port, as a percentage of total available bandwidth.

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

Traffic in Bytes:

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

Traffic in Frames:

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

Port Error Packet Statistics

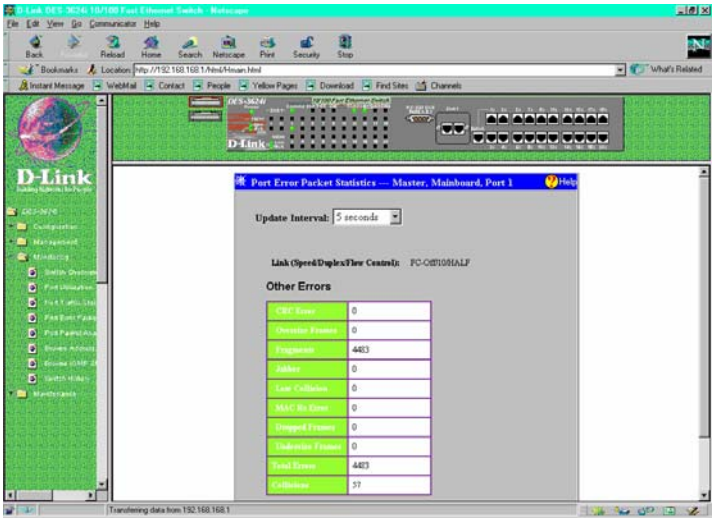


Figure 7-36. Port Error Packet Statistics window

The information is described as follows:

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

- **Link (Speed/Duplex/Flow Control)** 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 10BASE-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 best estimate of the total number of collisions on this Ethernet segment.

Port Packet Analysis Statistics

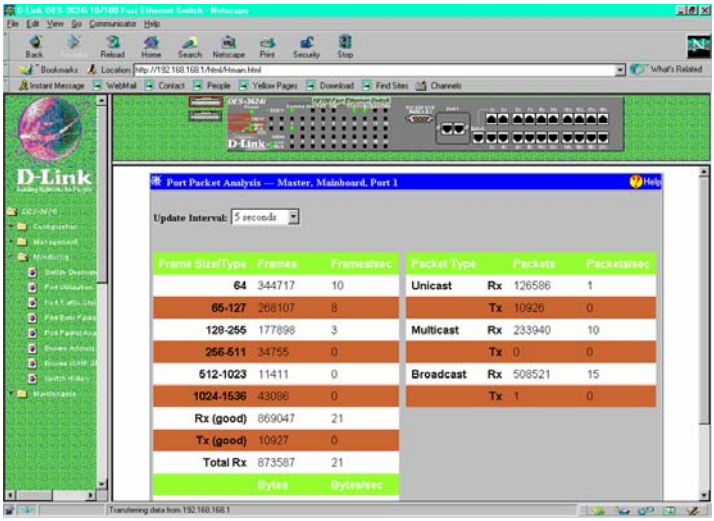


Figure 7-37. Port Packet Analysis window

The information is described as follows:

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

- **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

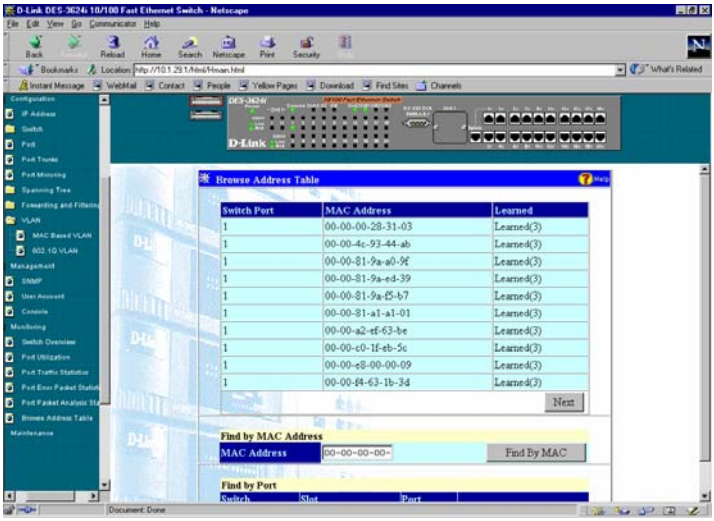


Figure 7-38. Browse Address Table window

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 **Find by MAC Address** or **Find by Port** sections above and then click the button on the right side of the section used.

Browse IGMP Status

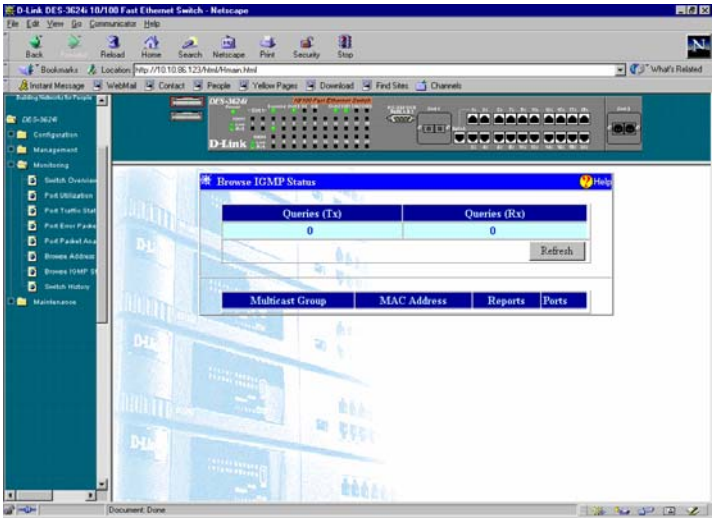


Figure 7-39. Browse IGMP Status window

This window allows you to enter the **Current 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 Group**, **MAC Address**, **Reports**, and **Ports** for IGMP Snooping in a table format.

Switch History

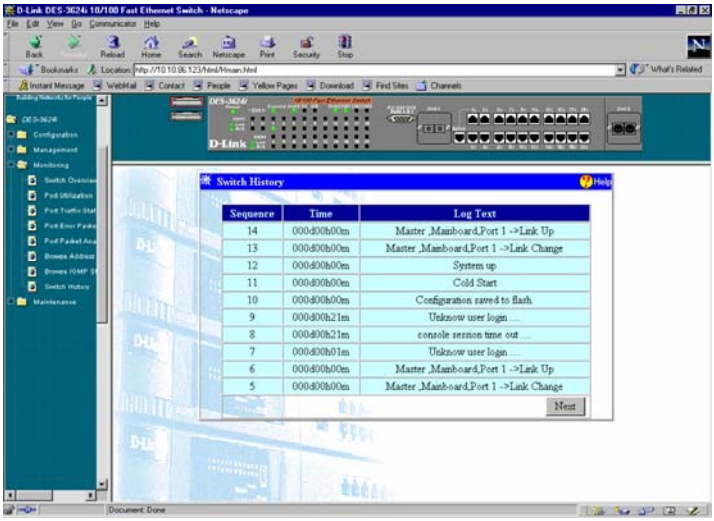


Figure 7-40. Switch History window

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.

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, Save Changes**, **Factory Reset**, and **Restart System**.

Firmware and Configuration Update

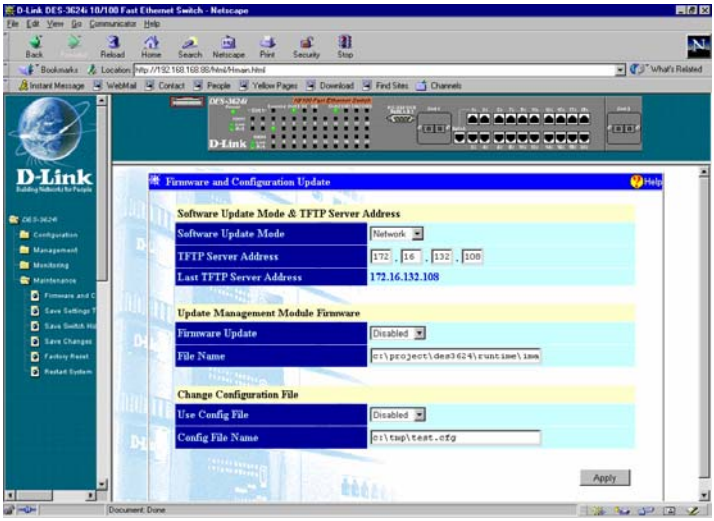


Figure 7-41. Firmware and Configuration Update window

To update firmware or change 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 should be obtained through the Ethernet network or through the console port.

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

- **Last TFTP Server Address** This read-only field displays the IP address of the last TFTP server accessed.

Update Management Module Firmware:

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

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

Change Configuration File:

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

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

Save Settings To TFTP Server

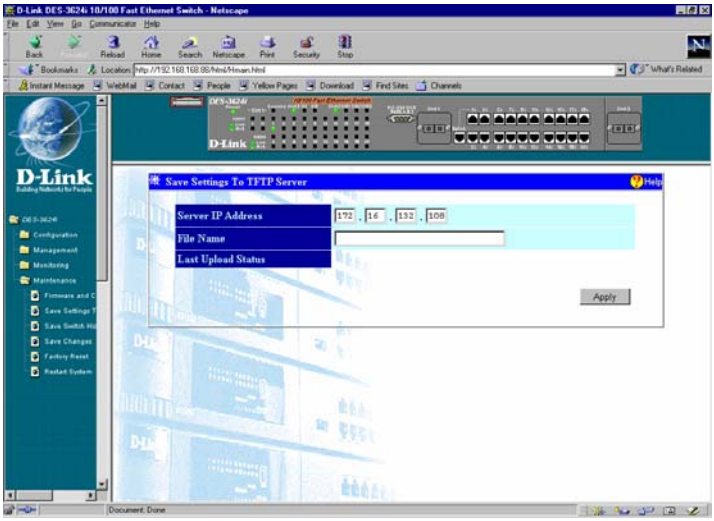


Figure 7-42. Save Settings To TFTP Server window

To upload a configuration file, enter the **Server IP Address** where the configuration file is located and the **File Name** and file path. Then click the **Apply** button.

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 configuration name on the TFTP server.
- **Last Upload Status** Shows whether the attempt to upload software was successful or not by displaying either "Success" or "Failed."

Save Switch History To TFTP Server

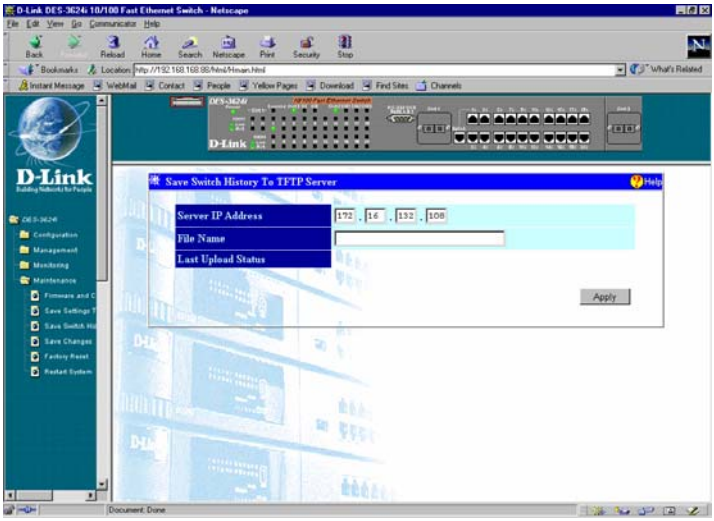


Figure 7-43. Save Switch History To TFTP Server window

To save a switch history file to your TFTP server, fill the fields in 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 "Failed".

Save Changes

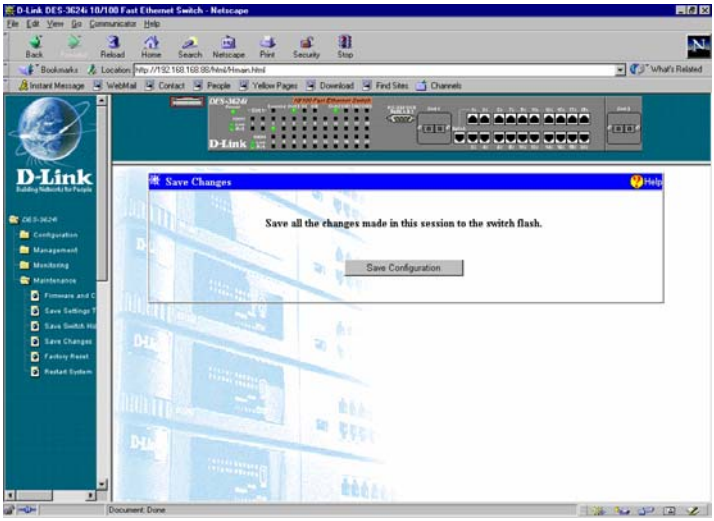


Figure 7-44. Save Changes window

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

Factory Reset

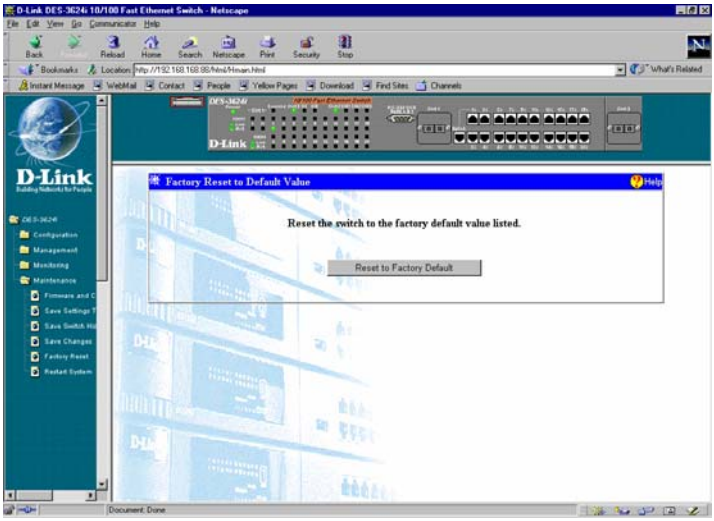


Figure 7-45. Factory Reset to Default Value window

Doing a remote reset is equivalent to turning the Switch off and on again. All parameters are returned to the values stored in EEPROM. Click the **Reset to Factory Default** button to initiate the reset.

Restart System

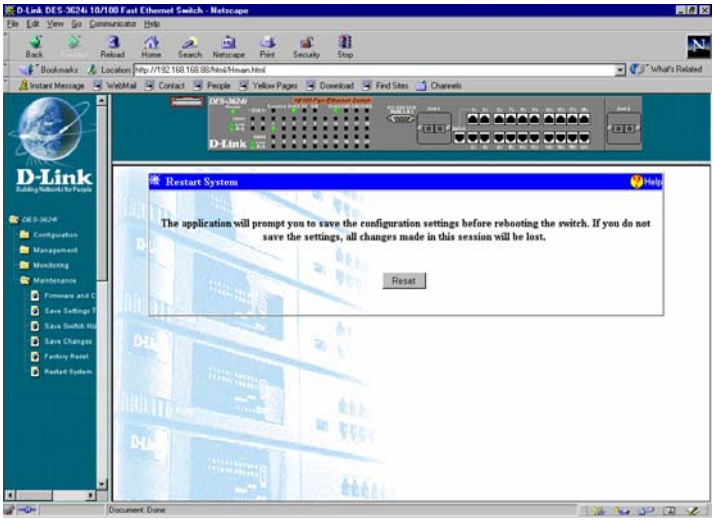


Figure 7-46. Restart System window

To perform a reboot of the Switch, which resets the system, click the **Reset** button.

A

TECHNICAL SPECIFICATIONS

General	
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE Ethernet IEEE 802.1 P/Q IEEE 802.3x
Protocol:	CSMA/CD
Data Transfer Rate:	Fast Ethernet: 100Mbps (half duplex) 200Mbps (full duplex)
Topology:	Star

General	
Network Cables:	10BASE-T: 2-pair UTP Cat. 3,4,5 (100 m) EIA/TIA- 568 100-ohm STP (100 m) 100BASE-TX: 2-pair or 4-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m) 100BASE-FX 50µm and 62.5µm multi-mode fiber 1000BASE-SX: 50µm and 62.5µm multi-mode fiber 1000BASE-LX: 50µm and 62.5µm multi-mode fiber or 10µm single-mode fiber
Number of Ports:	24x or 22x 10/100 Mbps NWay ports
Media Interface Exchange:	Connectors 1x and 2x in client devices are MDI-X jacks for ports 1 and 2. Connector 1x in the master device is an MDI-X jack for port 1.

Physical and Environmental	
AC inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)

Physical and Environmental	
Power Consumption:	46 watts maximum
DC fans:	2 built-in 40 x 40 mm fan
Operating Temperature:	0 to 50 degrees Celsius
Storage Temperature:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 367 mm x 44 mm (1U), 19 inch rack-mount width
Weight:	5 kg
EMI:	FCC Class A, CE Class A, VCCI Class A, BSMI Class A, C-Tick Class A
Safety:	UL, CSA, TUV/GS

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	12 Mbytes per device
Filtering Address Table:	12K MAC addresses per device (optimized condition)
Packet Filtering/Forwarding Rate:	148,800 pps per port (for 100Mbps)

Performance	
MAC Address Learning:	Aging time: 10 to 9999 seconds

B

RJ-45 PIN SPECIFICATION

When connecting the DES-3624 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.

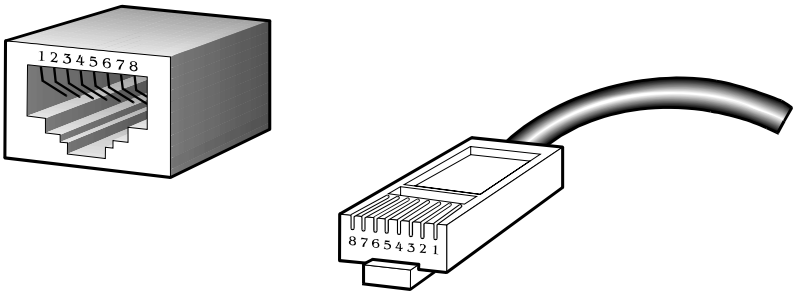


Figure B-1. The standard RJ-45 receptacle/connector

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:

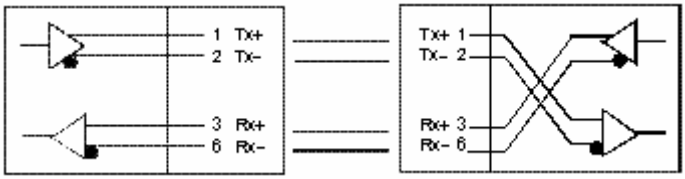


Figure B-2. Straight cable for Switch (uplink MDI-II port) to switch/Hub or other devices connection

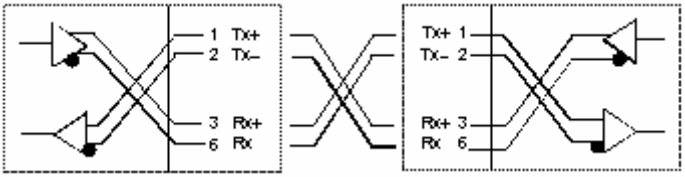


Figure B-3. Crossover cable for Switch (MDI-X port) to switch/hub or other network devices (MDI-X port) connection

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:\3624\3624prom.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:\3624\3624prom.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
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	Blank
Password	Blank
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	19 (Gigabit=4)
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	Default
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)
WEB: www.dlink.com.au E-MAIL: info@dlink.com.au

CANADA — **D-LINK CANADA**
2180 Winston Park Drive, Oakville, Ontario L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223
WEB: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca

CHILE — **D-LINK SOUTH AMERICA**
Isidora Goyenechea #2934 of.702, Las Condes, Santiago, Chile
TEL: 56-2-2323185 FAX: 56-2-2320923 WEB: www.dlink.cl

CHINA — **D-LINK CHINA**
15th Floor, Science & Technology Tower,
No. 11, Baishiqiao Road, Haidian District, Beijing 100081 China
TEL: 86-10-68467106-9 FAX: 86-10-68467110 WEB: www.dlink.co.cn

DENMARK — **D-LINK DENMARK**
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL:45-43-969-040 FAX:45-43-424-347 WEB: www.dlink.dk

EGYPT — **D-LINK MIDDLE EAST**
7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-2456176 FAX: 202-2456192 WEB: www.dlink-me.com

FRANCE — **D-LINK FRANCE**
Le FLORILEGE #2, Allee de la Fresnerie
78330 Fontenay Le Fleury France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689
WEB: www.dlink-france.fr E-MAIL: info@dlink-france.fr

GERMANY — **D-LINK GERMANY**
Bachstr. 22, D/65830 Kriftel Germany
TEL: 49-(0)6192-97110 FAX: 49-(0)6192-971111
WEB: www.dlink.de BBS: 49-(0)6192-971199 (Analog) 49-(0)6192-9711 98 (ISDN)
INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free)

INDIA — **D-LINK INDIA**
Plot No.5, Kurla-Bandra Complex Road,
Off Cst Road, Santacruz (E), Bombay - 400 098 India
TEL: 91-22-6526578 FAX: 91-22-6528476 WEB: www.dlink.india.com

ITALY — **D-LINK ITALY**
Via Nino Bonnet No. 6, 20154 Milano, Italy
TEL: 39-2-2900-0676 FAX: 39-2-2900-1723 E-Mail: dlink@tin.it

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

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

SWEDEN — **D-LINK SWEDEN**
World Trade Centre P. O. Box 70396, 107 24 Stockholm Sweden
TEL: 46-8-700-6211 FAX: 46-8-219-640 E-MAIL: info@dlink.se

TAIWAN — **D-LINK TAIWAN**
2F, No. 119 Pao-Chung Road, Hsin-Tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 WEB: www.dlinktw.com.tw

U.K. — **D-LINK EUROPE**
D-Link House, 6 Garland Road, Stanmore, London HA7 1DP U.K.
TEL: 44-181-235-5555 FAX: 44-181-235-5500
WEB: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. — **D-LINK U.S.A.**
53 Discovery Drive, Irvine, CA 92618 USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
WEB: www.dlink.com E-MAIL: tech@dlink.com

Registration Card

Print, type or use block letters.

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

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

(* Applies to adapters only)

Product was purchased from:
Reseller's name: _____
Telephone: _____ Fax: _____
Reseller's full address: _____
_____
_____

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

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

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

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

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

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

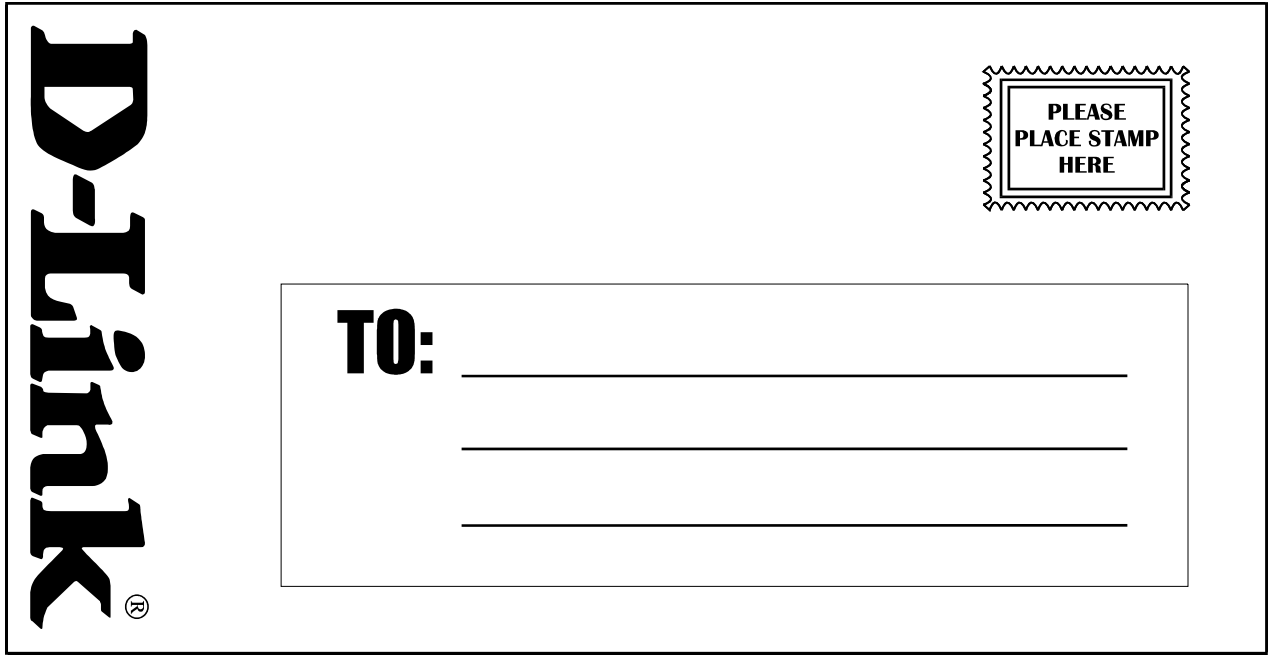
6. What network medium/media does your organization use ?
☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

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

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

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

10.Your comments on this product?
_____
_____


D-Link
PLEASE
PLACE STAMP
HERE
TO: