D-Link®

DES-3226S

Layer 2 Switch
Release III
User's Guide

Second Edition (April 2003)

651E3226S035

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 selection frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to selection 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 selection 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。

Table of Contents

1

INTRODUCTION

This section describes the functionality features of the DES-3226S. Some background information about Ethernet/Fast Ethernet, Gigabit Ethernet, and switching technology is presented.

Features

The DES-3226S Switch was designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continuously.

Switch features include:

Ports

- 24 high performance NWay ports all operating at 10/100 Mbps with Auto-MDIX function for connecting to end stations, servers and hubs.
- All ports can auto-negotiate (NWay) between 10Mbps/ 100Mbps, half-duplex or full duplex and flow control for half-duplex ports.
- One front panel slide-in module interface for a 2-port 1000BASE-SX, 1000BASE-LX, 1000BASE-T, 100BASE-FX, GBIC or 1-port GBIC & Stack module.

- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

Performance

- 24 built-in 10/100 Mbps ports
- Switch stacking configuration: 8 units per stack + 8 GBIC ports
- 1 open slot for 2 10/100 Mbps ports, 1 or 2 optional Fast Ethernet fiber or 2 Gigabit port (stand-alone configuration)
- 8.8 Gbps switching fabric capacity
- Auto MDI/MDIX uplink for all twisted-pair ports
- Supports 802.1Q VLAN, IGMP snooping, 802.1p Priority Queues, port mirroring
- Multi-layer ACL and QoS control
- Administrator-definable port security
- Port trunking of up to 8 Fast Ethernet ports
- 802.1D STP and 802.1w Rapid Spanning Tree for redundant back up bridge paths
- IEEE 802.3x Flow Control
- SNMP v.1, v.2, v.3 network management, RMON support
- 802.1x port access control
- Per-port bandwidth control
- IEEE 802.3z compliant for all Gigabit ports (optional)
- IEEE 802.3x compliant Flow Control support for all Gigabit ports (optional)

Management

- RS-232 console port for out-of-band network management via a console terminal or PC.
- IEEE 802.1w Rapid Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops.
- SNMP (v.1, v.2, v.3) Agent.
- IEEE 802.1X Support
- Port Security
- Fully configurable either in-band or out-of-band control via console serial connection.
- Flash memory for software upgrades. This can be done in-band via TFTP or out-of-band via the console. *Download the latest switch firmware from the D-Link website.*
- Built-in SNMP management:
    - Bridge MIB (RFC 1493)
    - MIB-II (RFC 1213)
    - Mini-RMON MIB (RFC 1757) – 4 groups
    - 802.1p MIB (RFC 2674).
    - IF MIB (RFC 2233)
    - Ether-Like MIB (RFC 1643)
- Supports Web-based management.
- CLI management support
- TFTP support.

- BOOTP support.
- DCHP Client support.

Switch Stacking

The DES-3226S can be used as a standalone or stacked switch – using the optional stacking module. Up to 8 Switches may be stacked and managed as a unit with a single IP address.

Management for the entire stack is done through the Master Switch.

You may add Switches later as needed.

Fast Ethernet Technology

100Mbps Fast Ethernet (or 100BASE-T) 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.

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 DES-3226S 24-port Fast Ethernet Layer 2 Switch
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This User's Guide with Registration Card

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

Installation

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

- The surface must support at least 3 kg
- The power outlet should be within 1.82 meters (6 feet) of the device
- Visually inspect the power cord and see that it is secured to the AC power connector
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch. Do not place heavy objects on the switch

Desktop or Shelf Installation

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

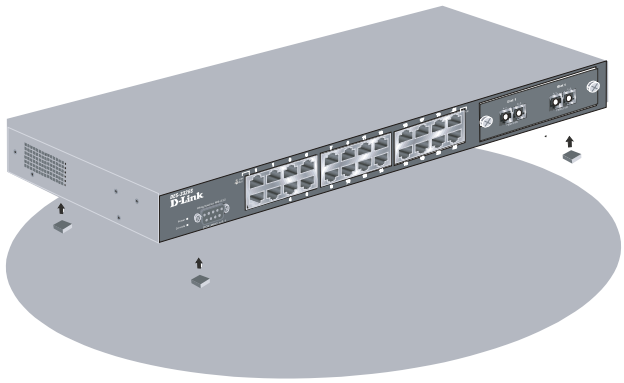


Figure 2-1. Installing rubber feet for desktop installation

Rack Installation

The DES-3226S can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.

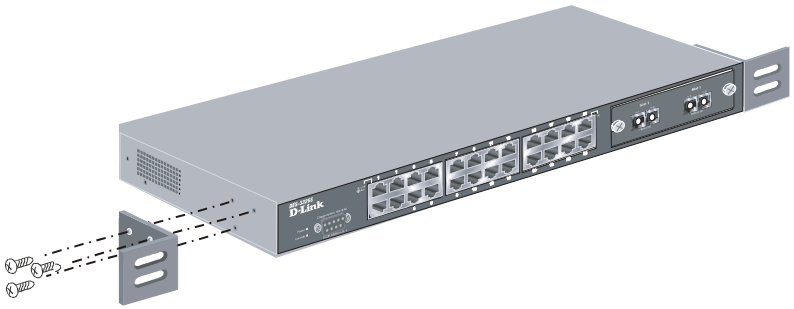


Figure 2- 2. Attaching the mounting brackets to the switch

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

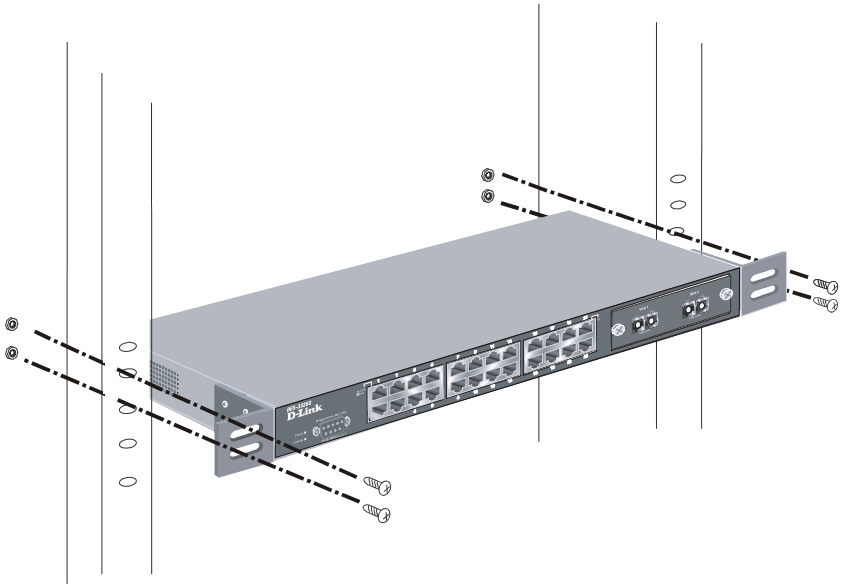


Figure 2-3. Installing the switch on an equipment rack

Power on

The DES-3226S switch can be used with AC power supply 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 is always on after the power is turned ON
- The console LED indicator will blink while the Switch loads onboard software and performs a self-test. 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 in the event of a power failure, unplug the switch. When the power supply is restored, 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 DES-3226S.

Front Panel

The front panel of the Switch consists of LED indicators, an RS-232 communication port, a slide-in module slot, and 24 (10/100 Mbps) Ethernet/Fast Ethernet ports.

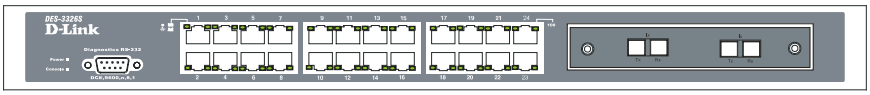


Figure 3 - 1. Front panel view of the Switch

- Comprehensive LED indicators display the status of the switch and the network (see the *LED Indicators* section below).
- An RS-232 DCE console port for setting up and managing the switch via a connection to a console terminal or PC using a terminal emulation program.

- A front-panel slide-in module slot for Gigabit Ethernet ports can accommodate a 2-port 1000BASE-T Gigabit Ethernet module, a 2-port 1000BASE-SX Gigabit Ethernet module, a 2-port 1000BASE-LX Gigabit Ethernet module, or a 2-port GBIC-based Gigabit Ethernet module.

- Twenty-four high-performance, NWay Ethernet ports all of which operate at 10/100 Mbps with Auto-MDIX function for connections to end stations, servers and hubs. All ports can auto-negotiate between 10Mbps or 100Mbps, full or half duplex, and flow control.

Rear Panel

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

Figure 3 - 2. Rear panel view of the Switch

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

Side Panels

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

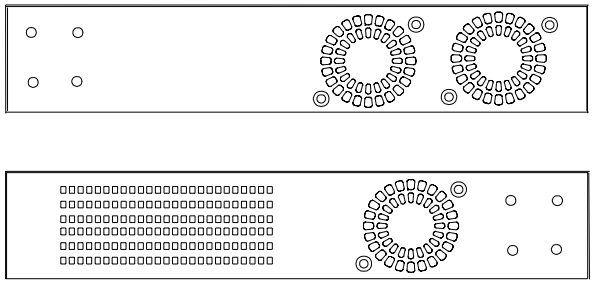


Figure 3 - 3. Side panel views of the Switch

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

Optional Plug-in Modules

The DES-3226S 24-port Fast Ethernet Switch is able to accommodate a range of optional plug-in modules in order to increase functionality and performance. These modules must be purchased separately.

100BASE-TX Module

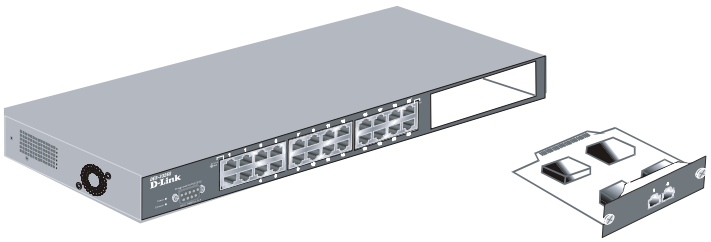


Figure 3 - 4. 1000BASE-TX two-port module

- IEEE802.3 10BASE-T/IEEE802.3u 100BASE-TX compliant
- Category 5e UTP cable connections of up to 100 meters.
- IEEE 802.3x compliant Flow Control support for full-duplex

100BASE-FX Fiber Module

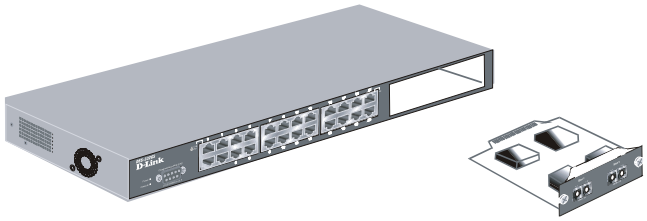


Figure 3-5. DES-132F 100BASE-FX two-port module

- Two 100BASE-FX (with SC type connector) Fiber ports
- Transmit distance up to 2 Km
- Fully compliant with IEEE802.3u
- Support Full-duplex operation only
- IEEE 802.3x compliant Flow Control support for full-duple

100BASE-FL Fiber Module

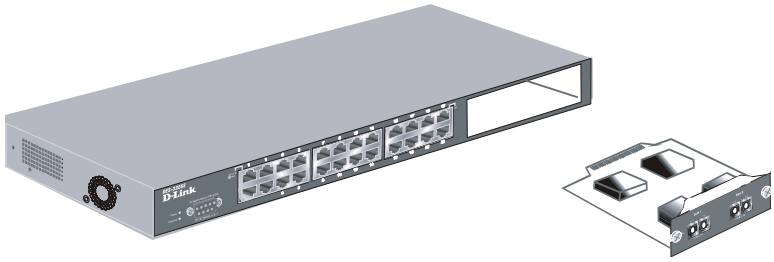


Figure 3 - 5. DES-132FL 100BASE-FX two-port module

- 100BASE-FX(SC-type connector) Ethernet Switch ports
- Transmit distance up to 15 Km
- IEEE802.3u 100BASE-FX compliant
- IEEE 802.3x compliant Flow Control support for full-duplex

1000BASE-T Module

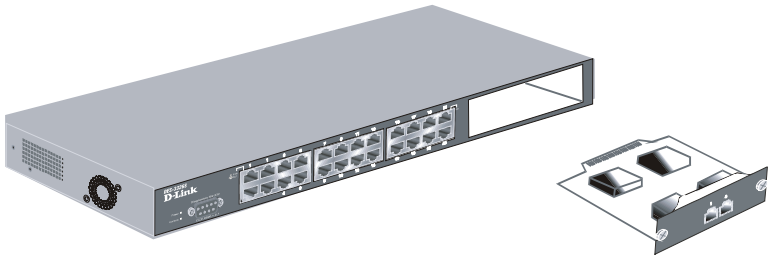


Figure 3 - 6. 1000BASE-TX two-port module

- Connects to 1000BASE-T devices
- Category 5e UTP cable connections of up to 100 meters.

1000BASE-SX Fiber Module

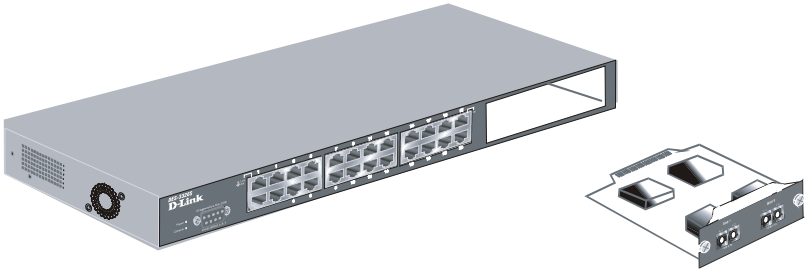


Figure 3 - 7. 1000BASE-SX two-port module

- Connects to 1000BASE-SX devices at full-duplex.
- Allows connections using multi-mode fiber optic cable in the following configurations:

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

1000BASE-LX Fiber Module

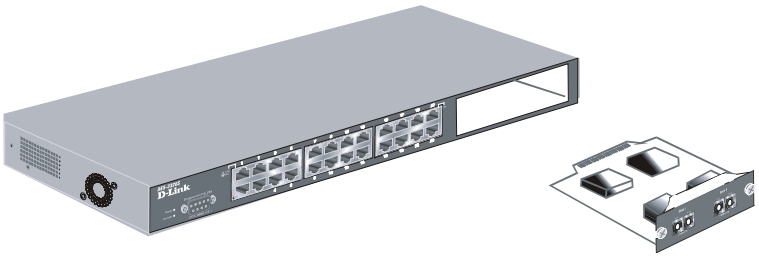


Figure 3 - 8. 1000BASE-LX two-port module

- Connects to 1000BASE-LX devices at full-duplex.
- Supports multi-mode fiber-optic cable connections of up to 550 meters or 5 km single-mode fiber-optic cable connections.

GBIC Two-Port Module

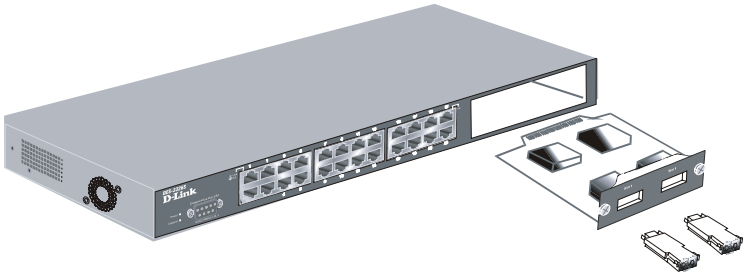


Figure 3 - 9. GBIC two-port module

- Connects to GBIC devices at full duplex only.
- Allows multi-mode fiber optic connections of up to 550 m (SX and LX) and single-mode fiber optic connections of up to 5 km (LX only). GBIC modules are available in –SX and –LX fiber optic media.
- IEEE 802.3x compliant Flow Control for full-duplex.

Stacking Module with GBIC Port

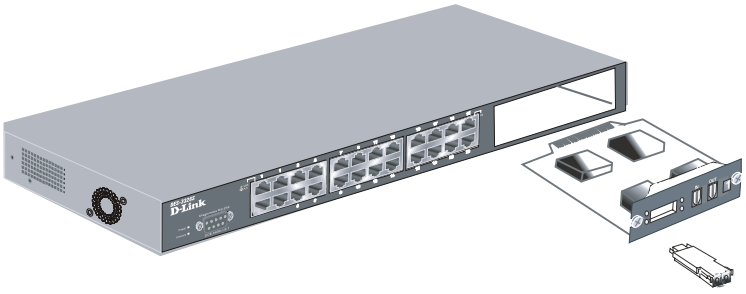


Figure 3 - 10. Stacking Module with one GBIC port

GBIC Port

- One Stacking port and one GBIC fiber port
- Connects to GBIC devices at full duplex only
- Allows multi-mode fiber optic connections of up to 550 m (SX) and single-mode fiber optic connections of up to 5 km (LX only). GBIC modules are available in –SX and –LX fiber optic media
- IEEE 802.3x compliant Flow Control for full-duplex

Stacking Port

- One transmitting port and one receiving port
- Use the connector of IEEE 1394b
- Data rate up to 1250 Mbps
- 7-segment LED display to indicate switch ID number within the switch stack

The optional Stacking Module allows up to eight DES-3226S Switches to be interconnected via their individual Stacking Modules. This forms an eight-switch stack that can then be managed and configured as thought the entire stack were a

single switch. The switch stack is then accessed through a single IP address or alternatively, through the master switch's serial port (via the management station's console and the switch's Command Line Interface).

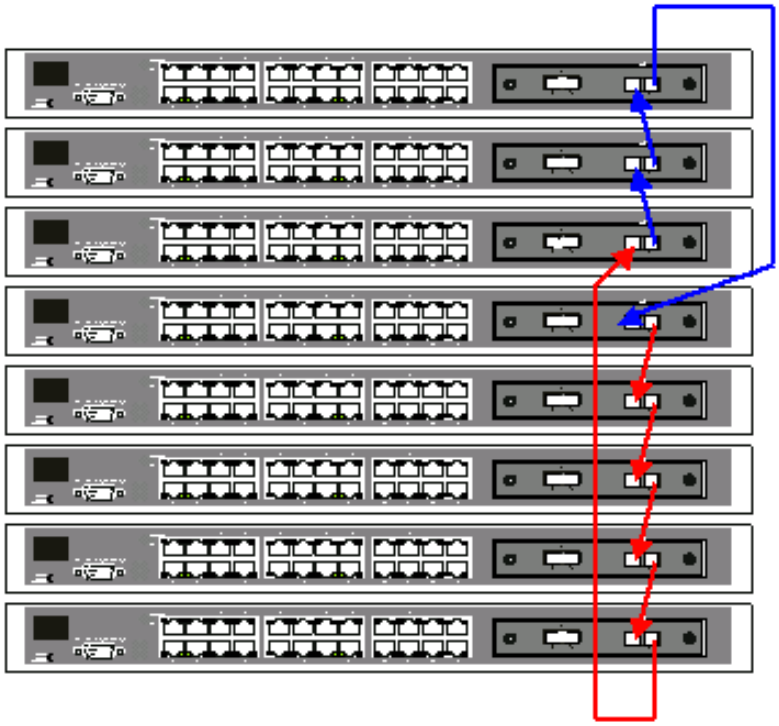


Figure 3 - 11. Up to 8 Switches in a Switch Stack

The stacking ports are marked **IN** and **OUT**. The IEEE 1394 compliant cable must be connected from an **IN** port on one switch to an **OUT** port on the next switch in the stack. The last two switches (at the top and bottom of the stack) must also be connected from the **IN** port on one switch to the **OUT** port on the other switch. In this way, a loop is made such that all of

the switches in the switch stack have the **IN** stacking port connected to another switch's **OUT** stacking port.

The Stacking Module's LED indicators are described below.

Switch LED Indicators

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

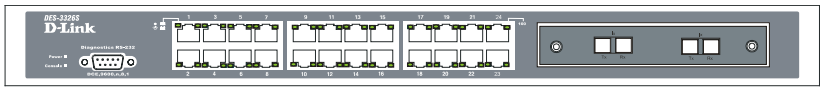


Figure 3 - 12. The LED Indicators

- **Power** This indicator on the front panel should be lit during the Power-On Self Test (POST). It will light green approximately 2 seconds after the switch is powered on to indicate the ready state of the device.

- **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.

- **Act/Link/Speed** These indicators are located to the left and right of each port. The right side indicator will light when the por has a link of 100 Mbps; the Link indicator will not light for 10 Mbps links. The LEDs blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.

Stacking Module LED Indicators

The switch's current order in the switch stack is also displayed on the Stacking Module's front panel – under the **STACK NO.** heading:

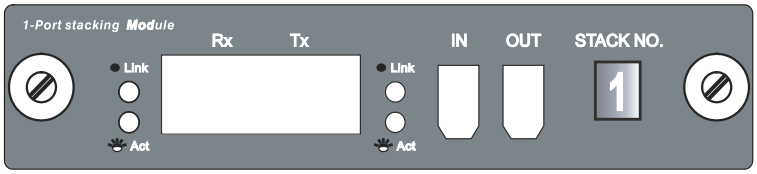


Figure 3 - 13. Stacking Module LED Indicators

The **Link** and **Act** LEDs have the same function as the corresponding LEDs for the switch's Ethernet ports. The **Link** LED lights to confirm a valid link, while the **ACT** LED blinks to indicate activity on the link.

The **Stack No.** seven-segment LED displays the Unit number assigned to the switch. A **0** (a **zero**) in the display indicates that the stacking module is in the process of determining the stack status and has not yet resolved the switch's Unit number.

The stacking order can be automatically configured using the switch's MAC address – the lower the numerical value of a given switch's MAC address, the lower the number in the stacking order the switch will be assigned. The switch with the lowest MAC address, will then become the Master Switch. This is the Stacking Module's default mode.

Alternatively, the stacking order can be manually assigned using the console's Command Line Interface (CLI) using the **config stacking mode** command.

4

CONNECTING THE SWITCH

This chapter describes how to connect the DES-3226S to your Fast Ethernet network.

Switch to End Node

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

An end node can be connected to the Switch via a two-pair Category 3, 4, 5 UTP/STP straight cable (be sure to use Category 5 UTP or STP cabling for 100 Mbps Fast Ethernet connections. Connections to 1000 Mbps Gigabit ports on the 1000BASE-T Module must also use Category 5e). The end node should be connected to any of the twenty-four ports of the DES-3326S.

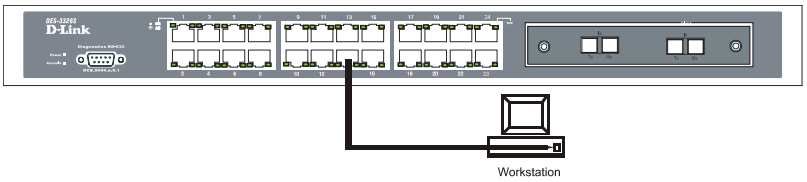


Figure 4-1. Switch connected to an End Node

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:

- The 100 LED indicator comes *ON* for a 100 Mbps and stays *OFF* for 10 Mbps.
- 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 at any port in either straight-through cable or a crossover cable because the switch supports Auto-MDIX function.

Note: Auto-MDIX function is not supported by the 100BASE-TX module.

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

Switch Stack Connections

Up to eight DES-3226S switches can be stacked, using the optional stacking module, into a switch stack that can then be configured and managed as a single unit. The Web-based Management agent of the Master Switch can configure and manage all of the switches in a switch stack – using a single IP address (the IP address of the Master Switch).

The Command Line Interface (CLI) can be also be used to manage and configure all of the switches in a switch stack – from the serial port on the master switch.

The CLI can also be used to configure and manage the switch stack via the TELNET protocol – using a single IP address (the IP address of the Master Switch).

The stacking ports are marked **IN** and **OUT**. The IEEE 1394 compliant cable must be connected from an **IN** port on one switch to an **OUT** port on the next switch in the stack. The last two switches (at the top and bottom of the stack) must also be connected from the **IN** port on one switch to the **OUT** port on the other switch. In this way, a loop is made such that all of the switches in the switch stack have the **IN** stacking port connected to another switch's **OUT** stacking port.

An example stacking port interconnection is shown below:

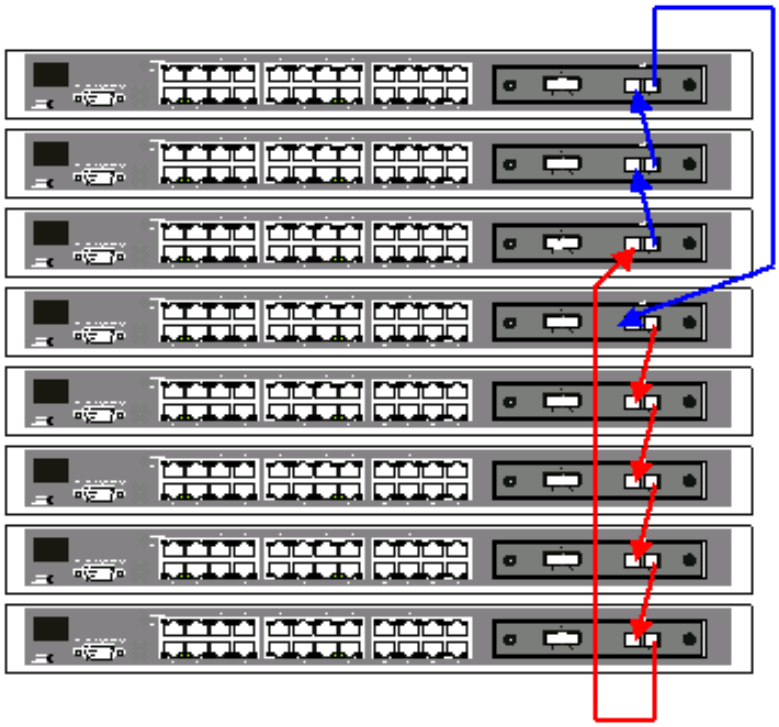


Figure 4-. Switch Stack connections between optional stacking modules

10BASE-T Device

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

- 100 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:

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

5

SWITCH MANAGEMENT AND OPERATING CONCEPTS

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

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

Local Console Management

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

Local console management uses the terminal connection to operate the console program built-in to the switch. A network administrator can manage, control and monitor the switch from the console program.

The DES-3226S contains a CPU, memory for data storage, flash memory for configuration data, operational programs, and SNMP agent firmware. These components allow the switch to be actively managed and monitored from either the console port or the network itself (out-of-band, or in-band).

Diagnostic (console) port (RS-232 DCE)

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) a to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management performed via management platforms, such as D-View, HP OpenView, etc. *Web-based Management* describes management of the switch performed over the network (in-band) using the switch's built-in Web-based management program (see Chapter 6 – Web-based Network Management). The operations to be performed and the facilities provided by these two built-in programs are identical.

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

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

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

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

Managing Switch Stacks

The Switch is designed to be stacked in stacks of up to six Switches, all managed as a single unit with a single IP address. The stack order is *hardware-determined*, that is, the unique MAC address of each Switch determines where the Switch stands in the stack order. This fact can be taken into account when you are placing the Switches in the equipment rack. Administrators may find it convenient to place the Switches in the rack in the same order they appear logically in the Switch stack. However, you also may prefer to override the auto-detect stack order feature if for example, you add Switches to a stack that is already in place. Regardless of the method used to determine Switch stack order, remember some important points:

- All management of all the Switches in the stack is done through the Master Switch
- It is recommended that the Master Switch be used to uplink to the Ethernet backbone
- If the link between any two switches fails or is disconnected, all of the switches in the stack will automatically reboot
- A switch stack has a single IP address – if the link to a given switch fails or is disconnected, that switch will reboot with the IP settings it had before becoming a member of the switch stack

- If a new Master is elected, all Switches in the stack will automatically reboot. This includes situations where the new Master is determined by MAC address, for example, if the original Master is removed from the stack.

- The Master Switch can be chosen automatically. Switch software auto-detects the MAC address of each Switch in the stack. The Switch with the lowest value MAC address is elected to function as the Master. The remaining Switches are ordered according to the relative value of their respective MAC addresses (see the following example).

Determining the Switch Stack Order

The example below illustrates adding a single switch to an installed stack of 5 switches. Using the auto-stacking mode, five MAC addresses appear in the order listed in the table below:

Stack Order	MAC Address
1(Master)	001122334451
2	001122334452
3	001122334453
4	001122334454
5	001122334455
6	Not in use

Table 5-1. Switch Stack Order – First

Now let us suppose you wish to add another Switch to this stack. The new Switch has a MAC address 001122334450. After rebooting all the Switches in the stack, the newly added Switch becomes the Master Switch. The new automatically determined stack order becomes:

Stack Order	MAC Address
1(added Switch)	001122334450
2(original Master)	001122334451
3	001122334452
4	001122334453
5	001122334454
6	001122334455

Table 5-2. Switch Stack Order – Second

You can override the automatic stack order selection to use the original Master Switch as the Master of the new stack (read *Switch Stacking Information* in Chapter 6 for information on how to override the stack order auto-detect function).

To override the automatic selection of the stack order you must attach the serial cable to the newly added Switch (MAC address 001122334450). Now you can reconfigure the stack to place the original Master Switch (MAC address 001122334451) again into the number 1 position and the newly added Switch into the number 6 position.

After reconfiguration and restarting the Switches, the new stack order becomes:

Stack Order	MAC Address
1(original Master)	001122334451
2	001122334452
3	001122334453
4	001122334454
5	001122334455
6 (added Switch)	001122334450

Table 5-3. Switch Stack Order – Final

Switch IP Address

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

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

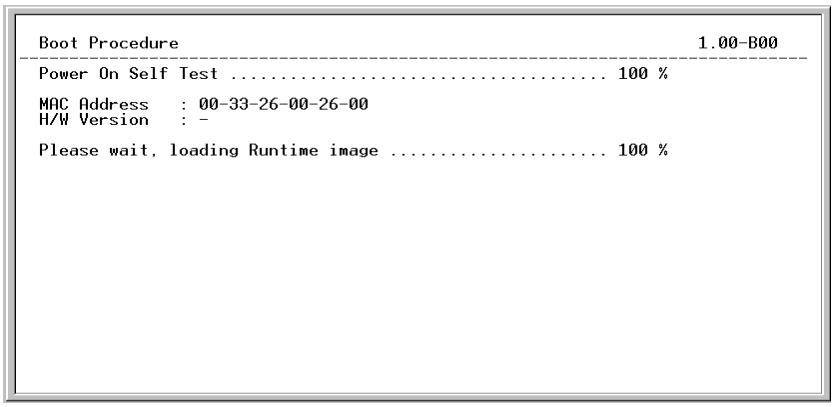


Figure 5-1. Console Boot Screen

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

Setting an IP Address

The IP address for the switch must be set before it can be managed with the web-based manager. The switch IP address may be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the switch must be known.

The IP address may alternatively be set using the Command Line Interface (CLI) over the console serial port as follows:

1. Starting at the command line prompt **DES3226S4#** – enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

2. Alternatively, you can enter **DES3226S4#** – enter the commands **config ipif system ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the ***z*** represents the corresponding number of subnets in CIDR notation.

Using this method, the switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the switch's web-based management agent.

Traps

Traps are messages that alert you of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port

status change. The Switch generates traps and sends them to the network manager (trap recipient).

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

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

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

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

- **Cold Start** This trap signifies that the Switch has been powered up and initialized such that software settings are reconfigured and hardware systems are rebooted. A cold start is different from a factory reset in that configuration settings saved to non-volatile RAM used to reconfigure the switch.

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

- **Authentication Failure** This trap signifies that someone has tried to logon to the switch using an invalid SNMP community string. The switch automatically stores the source IP address of the unauthorized user.

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

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

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

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

SNMP

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

SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol.

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

The DES-3226S has a software program called an 'agent' that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

Authentication

The authentication protocol ensures that both the router SNMP agent and the remote user SNMP application program discard packets from unauthorized users. Authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the router SNMP must use the same community string. SNMP community strings of up to 32 characters may be entered under the *Remote Management Setup* menu of the console program.

Traps

Traps are messages that alert network personnel 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 trap recipient (or network manager).

Trap recipients are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap recipients will receive traps sent from the

Switch; they must immediately take certain actions to avoid future failure or breakdown of the network.

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

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

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

- **Cold Start** This trap signifies that the Switch has been powered up and initialized such that software settings are reconfigured and hardware systems are rebooted. A cold start is different from a factory reset in that configuration settings saved to non-volatile RAM used to reconfigure the switch.

- **Authentication Failure** This trap signifies that someone has tried to logon to the switch using an invalid SNMP community string. The switch automatically stores the source IP address of the unauthorized user.

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

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

MIBs

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

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

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

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

Packet Forwarding

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

MAC Address Aging Time

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

The aging time can be from 300 to 1,000,000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the switch.

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

Static forwarding entries are not affected by the aging time.

Filtering

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

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

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

Some filtering is done automatically by the switch:

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

Some filtering requires the manual entry of information into a filtering table:

- MAC address filtering – the manual entry of specific MAC addresses to be filtered from the network. Packets sent from one manually entered MAC address can be filtered from the network. The entry may be specified as either a source, a destination, or both.

- IP address filtering – the manual entry of specific IP addresses to be filtered from the network (switch must be in IP Routing mode). Packets sent from one manually entered IP address to another can be filtered from the network. The entry may specified as either a source, a destination, or both (switch must be in IP Routing mode).

802.1w Rapid Spanning Tree

The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEE 802.1w specification and a version compatible with the IEEE 802.1d STP. RSTP can operate with legacy equipment implementing IEEE 802.1d, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 function that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the two protocols is in the way ports transition to a forwarding state and the in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. RSTP combines the transition states disabled, blocking and listening used in 802.1d and creates a single state *Discarding*. In either case, ports do not forward packets; in the STP port transition states disabled, blocking or listening or in the RSTP port state discarding there is no functional difference, the port is not active in the network topology. Table 5-7 below compares how the two protocols differ regarding the port state transition.

Both protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All

bridges listen for BPDU packets. However, BPDU packets are sent more frequently – with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges are sensitive to the status of the link. Ultimately this difference results faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1d is this absence of immediate feedback from adjacent bridges.

802.1d STP	802.1w RSTP	Forwarding?	Learning?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

Table 5-5. Comparing Port States

RSTP is capable of more rapid transition to a forwarding state – it no longer relies on timer configurations – RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports, transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its

status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1d/802.1w Compatibility

RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1d format when necessary. However, any segment using 802.1 STP will not benefit from the rapid transition and rapid topology change detection of RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP.

Link Aggregation

Link aggregation 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 link aggregation group, with one port designated as the **master port** of the group. Since all members of the link aggregation group must be configured to operate in the same manner, the configuration of the master port is applied to all members of the link aggregation group. Thus, when configuring the ports in a link aggregation group, you only need to configure the master port.

The DES-3226S supports link aggregation groups, which may include from 2 to 8 switch ports each, except for a Gigabit link aggregation group which consists of the 2 (optional) Gigabit Ethernet ports of the front panel. These ports are the two

1000BASE-SX, -LX –TX or GBIC ports contained in a front-panel mounted module.

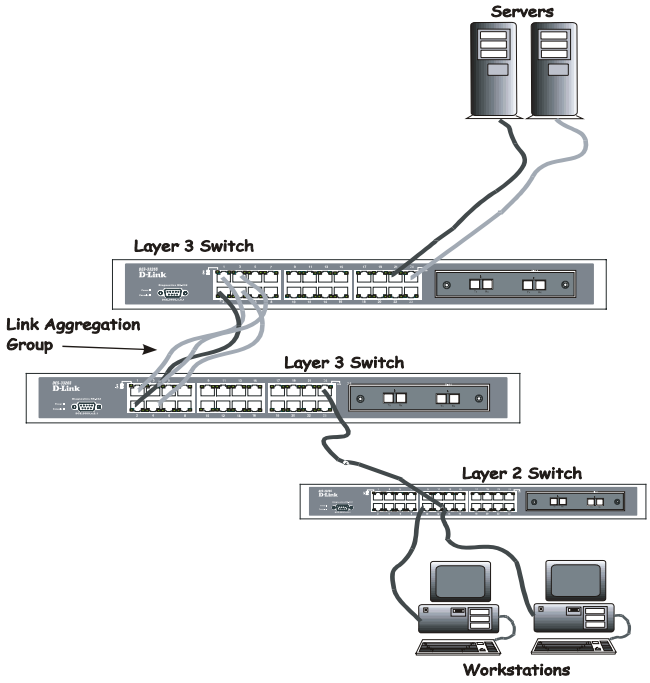


Figure 5-2. Link Aggregation Group

Data transmitted to a specific host (destination address) will always be transmitted over the same port in a link aggregation group. This allows packets in a data stream to arrive in the same order they were sent. A aggregated link connection can be made with any other switch that maintains host-to-host data streams over a single link aggregate port. Switches that use a load-balancing scheme that sends the packets of a host-to-host data stream over multiple link aggregation ports cannot have a aggregated connection with the DES-3226S switch.

VLANs

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

IEEE 802.1Q VLANs

Some relevant terms:

Tagging - The act of putting 802.1Q VLAN information into the header of a packet.

Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

Ingress port - A port on a switch where packets are flowing into the switch and VLAN decisions must be made.

Egress port - A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the DES-3226S switch. 802.1Q VLANs require tagging, which enables the VLANs to span an entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

Any port can be configured as either *tagging* or *untagging*. The *untagging* feature of IEEE 802.1Q VLANs allow VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The *tagging* feature allows VLANs to span multiple 802.1Q VLAN compliant switches through a single physical

connection and allows Spanning Tree to be enabled on all ports and work normally.

802.1Q VLAN Packet Forwarding

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

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

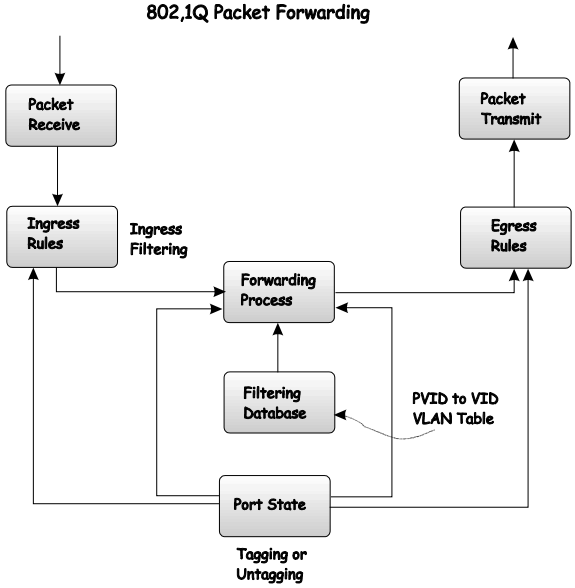


Figure 5-3. IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

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

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

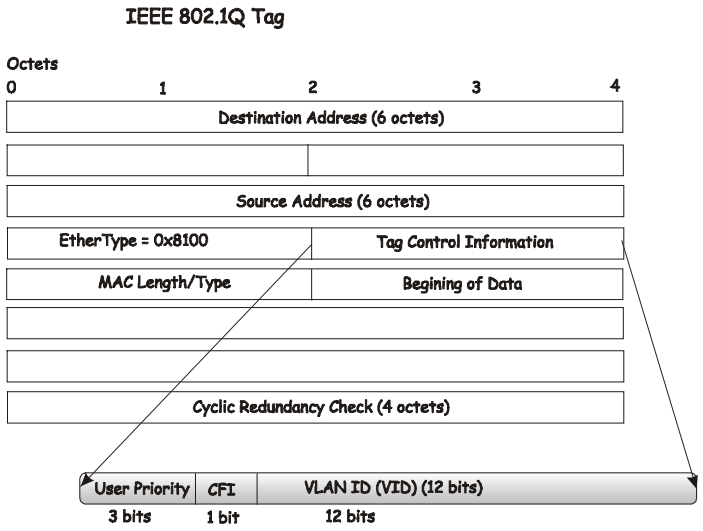


Figure 5-4. IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

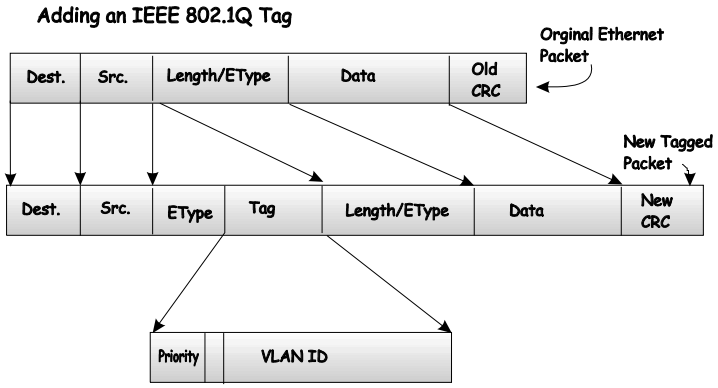


Figure 5-5. Adding an IEEE 802.1Q Tag

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as *tag-unaware.* 802.1Q devices are referred to as *tag-aware.*

Prior to the adoption 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be

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

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

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

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

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

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be

transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

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

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

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

Ingress Filtering

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

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the

ingress port is a member of the 802.1Q VLAN, the switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

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

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

Multicasting

Multicasting is a group of protocols and tools that enable a single source point to send packets to groups of multiple destination points with persistent connections that last for some amount of time. The main advantage to multicasting is a decrease in the network load compared to broadcasting.

Multicast Groups

Class D IP addresses are assigned to a group of network devices that comprise a multicast group. The four most

significant four bits of a Class D address are set to "1110". The following 28 bits is referred to as the 'multicast group ID'. Some of the range of Class D addresses are registered with the Internet Assigned Numbers Authority (IANA) for special purposes. For example, the block of multicast addresses ranging from 224.0.0.1 to 224.0.0.225 is reserved for use by routing protocols and some other low-level topology discovery and maintenance protocols.

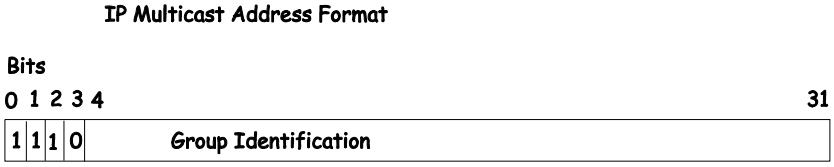


Figure 5-6. Class D Multicast Address

Some of the reserved IP multicast addresses are as follows:

Address	Assignment
224.0.0.0	Base Address (reserved)
224.0.0.1	All Systems on this subnet
224.0.0.2	All Routers on this subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPF IGP Routers
224.0.0.6	OSPF IGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	All RIP2 Routers
224.0.0.10	All IGRP Routers
224.0.0.11	Mobile Agents
224.0.0.12	DHCP Servers and Relay Agents
224.0.0.13	All PIM Routers
224.0.0.14	RSVP Encapsulation
224.0.0.15	All CBT Routers
224.0.0.16	Designated Sbm
224.0.0.17	All Sbms
224.0.0.18	VRRP
224.0.0.19 through 224.0.0.225	Unassigned
224.0.0.21	DVMRP on MOSPF

Table 5-6. Reserved Multicast Address Assignment

Internet Group Management Protocol (IGMP)

End users that want to receive multicast packets must be able to inform nearby routers that they want to become a multicast group member of the group these packets are being sent to. The Internet Group Management Protocol (IGMP) is used by multicast routers to maintain multicast group membership. IGMP is also used to coordinate between multiple multicast routers that may be present on a network by electing one of the multicast routers as the 'querier'. This router then keep track of the membership of multicast groups that have active members on the network. IGMP is used to determine whether the router should forward multicast packets it receives to the subnetworks it is attached to or not. A multicast router that has received a multicast packet will check to determine if there is at least one member of a multicast group that has requested to receive multicast packets from this source. If there is one member, the packet is forwarded. If there are no members, the packet is dropped.

IGMP Versions 1 and 2

Users that want to receive multicast packets need to be able to join and leave multicast groups. This is accomplished using IGMP.

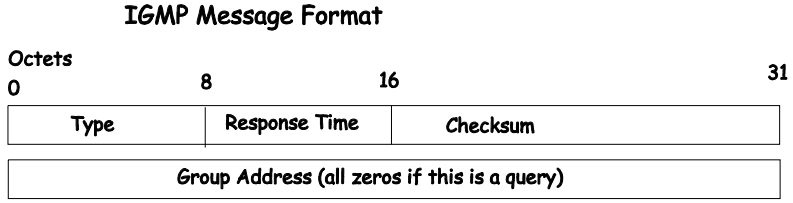


Figure 5-7 IGMP Message Format

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

Table 5-7. IGMP Type Codes

Multicast routers use IGMP to manage multicast group memberships:

- An IGMP "report" is sent by a user's computer to join a group
- IGMP version 1 does not have an explicit 'leave' message. Group members have an expiration timer, and if this timer expires before a query response is returned, the member is dropped from the group.
- IGMP version 2 introduces an explicit "leave" report. When a user wants to leave a group, this report is sent to the multicast router (for IGMP version 2).
- Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their subnetworks. If there is no response from a particular group, the router assumes that there are no group members on the network, and multicast packets are not forwarded.

The TTL field of query messages is set to 1 so that the queries do not get forwarded to other subnetworks.

IGMP version 2 introduces a few extensions to IGMP version 1 such as, the election of a single multicast querier for each network, explicit 'leave' reports, and queries that are specific to a particular multicast group.

The router with the lowest IP address is elected as the querier. The explicit group leave message is added to decrease latency, and routers can ask for membership reports from a particular multicast group ID.

The transition states a host will go through to join or leave a multicast group are shown in the diagram below.

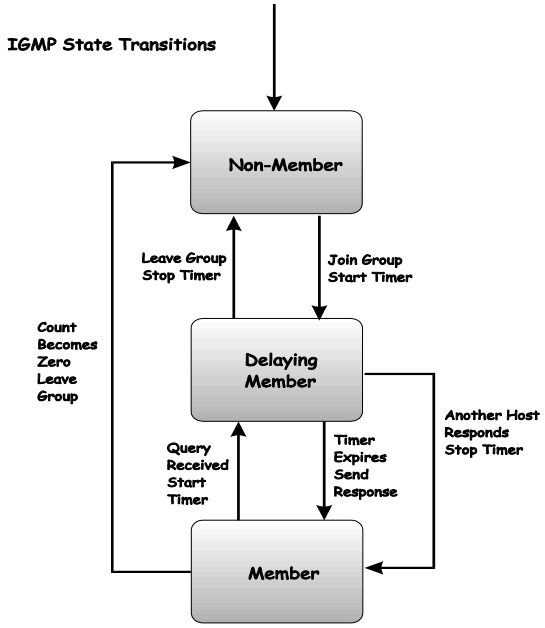


Figure 5-8 IGMP State Transitions

6

WEB-BASED SWITCH MANAGEMENT

Introduction

The DES-3226S offers an embedded Web-based (HTML) interface allowing users to manage the switch from anywhere on the network through a standard browser such as Netscape Navigator/Communicator or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

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

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

Getting Started

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

The second step is to configure an IP interface on the Switch. This can be done manually through the console or automatically using BOOTP/DHCP.

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.

Note: The Factory default IP address for the switch is 10.90.90.90.

In the page that opens, click on the **Login to make a setup** button:

Figure 6 - 1. Login Button

This opens the management module's main page.

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

Configuring the Switch

User Accounts Management

From the **Main Menu**, highlight S**etup User Accounts** and press Enter, then the **User Account Management** menu

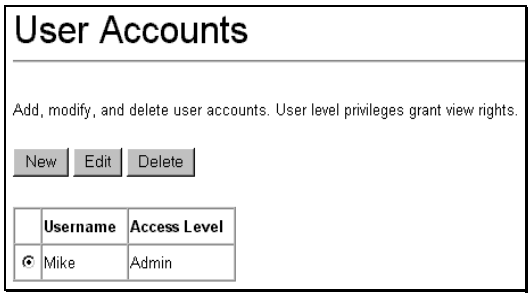


Figure 6 - 2. User Accounts Control Table

Click **New** to add a user.

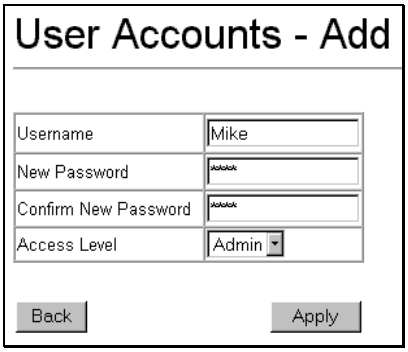


Figure 6 - 3. User Accounts Control Table - Add

1. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have **Admin** or **User** privileges.

2. Click on **APPLY** to make the user addition effective.
3. A listing of all user accounts and access levels is shown on the user accounts control table. This list is updated when Apply is executed.
4. Please remember that Apply makes changes to the switch configuration for the ***current session only.*** ***A***ll changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the **Main Menu** - if you want these changes to be permanent.

Admin and User Privileges

There are two levels of user privileges: *Admin* and *User*. Some menu selections available to users with *Admin* privileges may not be available to those with *User* privileges.

The following table summarizes the *Admin* and *User* privileges:

Sw tch Configuration Ma agement	***Privile ge***	
	Admin	***User***
Configuration	Yes	Read Only
Network Monitoring	Yes	Read Only
Community Strings and Trap Stations	Yes	Read Only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	Ping Only
Factory Reset	Yes	No
Reboot Switch	Yes	No
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

Table 6-1. Admin and User Privileges

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

Saving Changes

The DES-3226S has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by highlighting `Apply` and pressing 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 erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

To retain any configuration changes permanently, highlight **Save Changes** from the **Main Menu**. The following screen will appear:

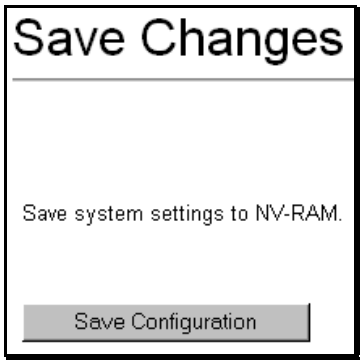


Figure 6 - 4. Save Changes Screen

Click the **Save Configuration** button to save the current switch configuration in NV-RAM. The following dialog box will confirm that the configuration has been saved:

Figure 6 - 5. Save Configuration Confirmation

Click the **OK** button to continue.

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

Factory Reset

The **Factory Reset** function has several options when resetting the switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

Note: only the **Reset System** option will enter the factory default parameters into the switch's non-volatile RAM, and then restart the switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. **Reset System** will return the switch's configuration to the state it was when it left the factory.

Reset gives the option of retaining the switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the switch is reset with this option enabled, and **Save Changes** is not executed, the switch will return to the last saved configuration when rebooted.

The **Reset Config** option will reset all of the switch's configuration parameters to their factory defaults, without saving these default values to the switch's non-volatile RAM. If the switch is reset with this option enabled, and **Save Changes** is not executed, the switch will return to the last saved configuration when rebooted.

In addition, the **Reset System** option is added to reset all configuration parameters to their factory defaults, save these parameters to the switch's non-volatile RAM, and then restart the switch. This option is equivalent to **Reset Config** (above) followed by **Save Changes**.

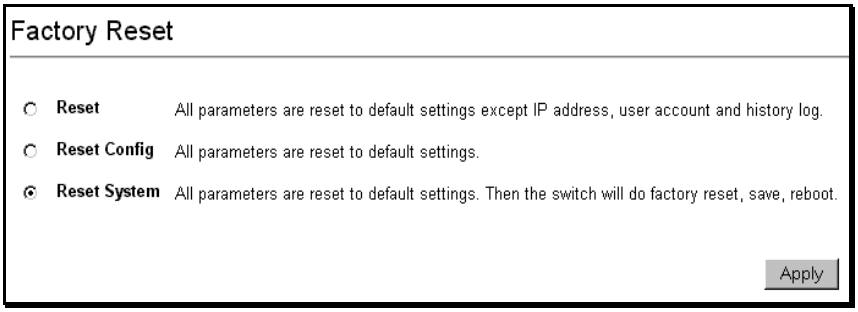


Figure 6 - 6. Factory Reset Screen

Click the **Apply** button to reset the switch.

Restart System

The following menu is used to restart the switch.

Clicking the **Yes** click-box will instruct the switch to save the current configuration to non-volatile RAM before restarting the switch.

Clicking the **No** click-box instructs the switch not to save the current configuration before restarting the switch. All of the configuration information entered from the last time **Save Changes** was executed, will be lost.

Note: clicking **Yes** is equivalent to executing **Save Changes** and then restarting the switch.

Click the **Restart** button to restart the switch.

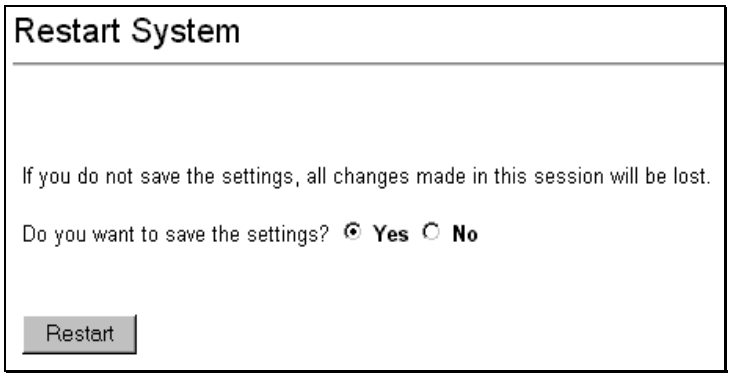


Figure 6 - 7. Restart System Screen

Web-based Manager's User Interface

The user interface provides access to various switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into 3 distinct areas as described in the table.

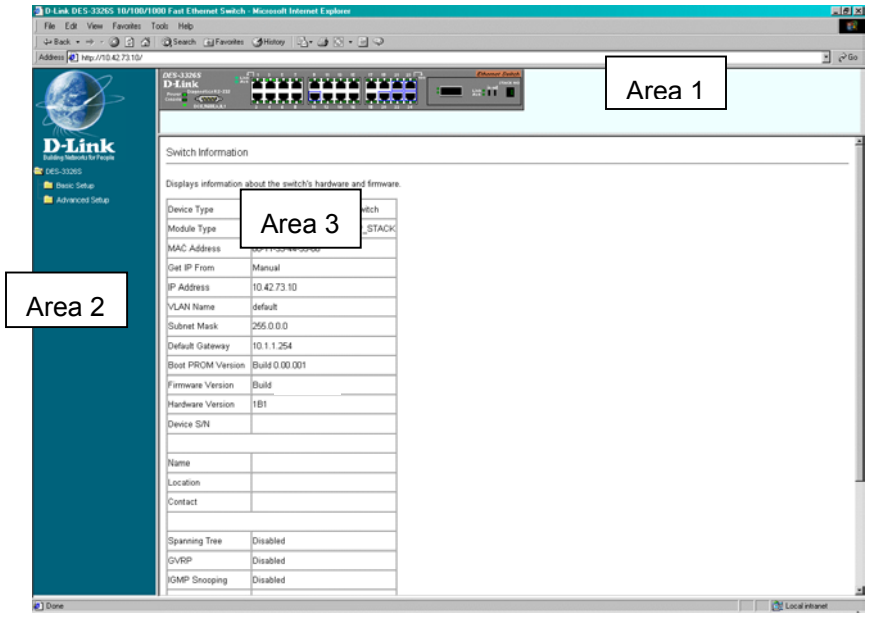


Figure 6 - 8. Main Web-Manager Screen

Area	Function
1	Presents a graphical near real-time image of the front panel of the switch. This area displays the switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including the

ports, expansion modules, management module, or the case.

2 Allows the selection of commands.

3 Presents switch information based on your selection and the entry of configuration data.

This section, arranged by topic, describes how to perform common monitoring and configuration tasks on the DES-3226S switch using the Web-based Manager, you can perform any of the tasks described in the following sections.

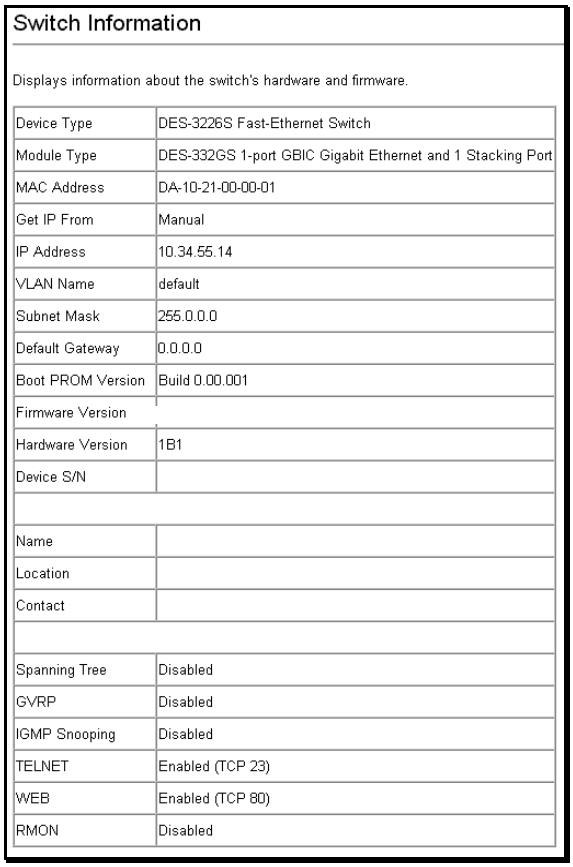
Setting Up the Switch

Basic Setup

This section will help prepare the Switch user by describing the Switch Information – Basic Settings, IP Address, Configure Port, and Switch Settings windows.

Switch Information

Click the **Switch Information** link in the **Configuration** menu.



Switch Information

Displays information about the switch's hardware and firmware.

Device Type	DES-3226S Fast-Ethernet Switch
Module Type	DES-332GS 1-port GBIC Gigabit Ethernet and 1 Stacking Port
MAC Address	DA-10-21-00-00-01
Get IP From	Manual
IP Address	10.34.55.14
VLAN Name	default
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
Boot PROM Version	Build 0.00.001
Firmware Version	
Hardware Version	1B1
Device S/N	
Name	
Location	
Contact	
Spanning Tree	Disabled
GVRP	Disabled
IGMP Snooping	Disabled
TELNET	Enabled (TCP 23)
WEB	Enabled (TCP 80)
RMON	Disabled

Figure 6 - 9. Switch Information – Basic Settings

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

Configuring the Switch's IP Address

The Switch needs to have an IP address assigned to it so that an In-Band network management system (for example, the Web Manager or Telnet) client can find it on the network. The **Basic Switch Setup** window allows you to change the settings for the Ethernet interface used for in-band communication.

The fields listed under the **Current IP Settings** heading are those that are currently being used by the switch. Those fields listed under the **New Switch IP Setting** heading are those that will be used after clicking on the **Apply** button.

To set the switch's IP address:

Click the **Basic Switch Setup** link from the **Main Menu** to open the following dialog box.

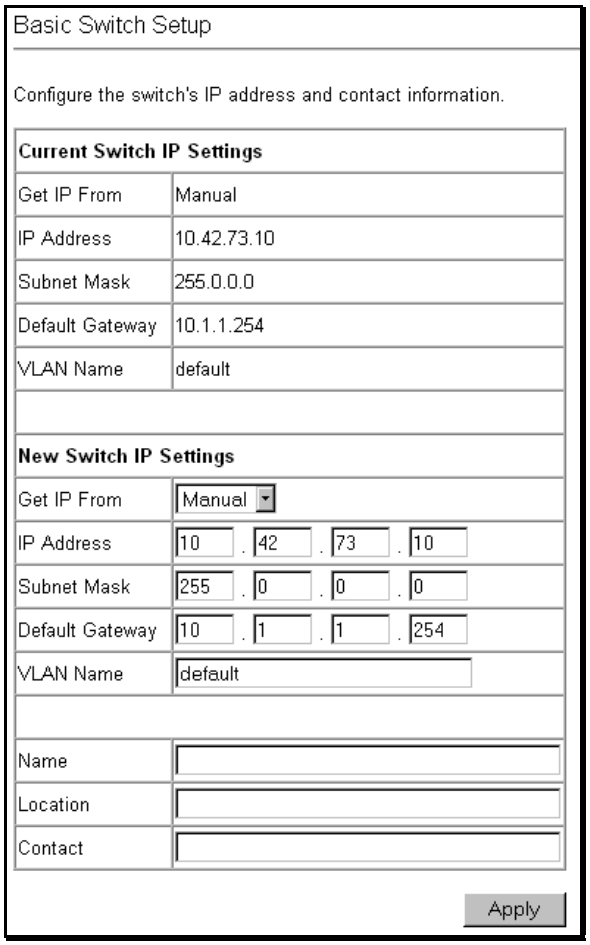


Figure 6 - 10. Basic Switch Setup

Note: the switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

To manually assign the switch's IP address, subnet mask, and default gateway address:

Select **Manual** from the **Get IP From** drop-down menu.

Enter the appropriate IP address and subnet mask.

If you want to access the switch from a different subnet from the one it is installed on, enter the IP address of the gateway. If you will manage the switch from the subnet on which it is installed, you can leave the default address in this field.

If no VLANs have been previously configured on the switch, you can use the default VLAN – named **default**. The default VLAN contains all of the switch ports as members. If VLANs have been previously configured on the switch, you will need to enter the VLAN name of the VLAN that contains the port that the management station will access the switch on.

To use the BOOTP or DHCP protocols to assign the switch an IP address, subnet mask, and default gateway address:

Use the **Get IP From: <***Manual***>** pull-down menu to choose from *Manual*, *BOOTP*, or *DHCP*. This selects how the switch will be assigned an IP address on the next reboot (or startu*p*).

The **New Switch IP Settings** options are:

Parameter	Description
BOOTP	The switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.

DHCP	The switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
Manual	Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the switch. These fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields which require entries under this option are as follows:
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.

Default Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
VLAN Name	This allows the entry of a VLAN name from which a management station (a computer) will be allowed to manage the switch using TCP/IP (in-band, or over the network). Management stations that are on VLANs other than the one entered in the **VLAN Name** field will not be able to manage the switch in-band unless their IP addresses are entered in the **Management Station IP Addresses** field. The default VLAN is named **default** and contains all of the switch's ports. There are no entries in the **Management Station IP Addresses** table, by default – so any management station can access the switch.

Stacking Information

To change a switch's default stacking configuration (for example, the order in the stack), you must use the console Command Line Interface.

The number of switches in the switch stack (up to 8 – total) are displayed in the upper right-hand corner of you web-browser. The icons are in the same order as their respective Unit numbers, with the Unit 1 switch corresponding to the icon in the upper left-most corner of the icon group.

When the up to 8 DES-3226S switches are properly interconnected through their optional Stacking Modules, information about the resulting switch stack is displayed under the **Stack Information** link. This link is visible only when a switch stack has been connected and the optional Stacking Modules are active.

To view the stacking information, click on the Stacking Information link from the Basic Setup folder:

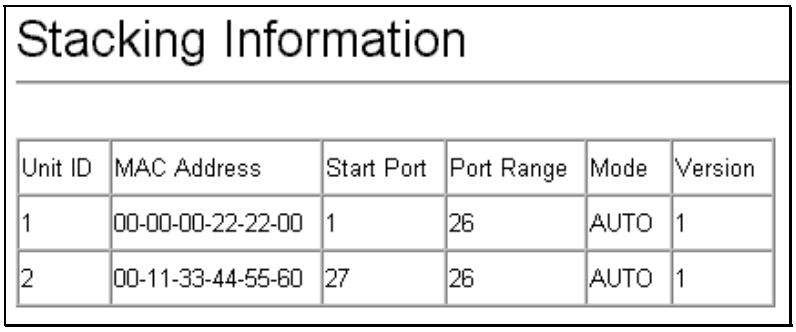


Figure 6 - 11. Stacking Information

The **Unit ID** field displays the switch's order in the stack. The switch with a Unit ID of 1 is the Master Switch.

The **MAC Address** field displays the unique address of the switch assigned by the factory.

The **Start Port** field displays the first port assigned to the corresponding switch in the switch stack.

The **Port Range** field displays the total number of ports on the switch. Note that the stacking port is included in the total count.

Mode displays the method used to determine the stacking order of the switches in the switch stack.

The **Version** field displays the version number of the stacking firmware.

The switch's current order in the switch stack is also displayed on the Stacking Module's front panel – under the **STACK NO.** heading:

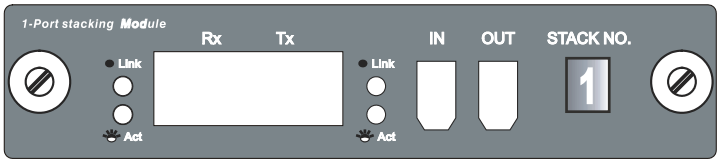


Figure 6 - 12. The Stacking Module's Front Panel

Notice the **Link** and **Act** LEDs. These LEDs have the same function as the corresponding LEDs for the switch's Ethernet ports. The **Link** LED lights to confirm a valid link, while the **ACT** LED blinks to indicate activity on the link.

The **Stack No.** seven-segment LED displays the Unit number assigned to the switch. A **0** (a **zero**) in the display indicates that the stacking module is in the process of determining the stack status and has not yet resolved the switch's Unit number.

The stacking order can be automatically configured using the switch's MAC address – the lower the numerical value of a given switch's MAC address, the lower the number in the stacking order the switch will be assigned. The switch with the lowest MAC address, will then become the Master Switch.

Alternatively, the stacking order can be manually assigned using the console's Command Line Interface (CLI).

You can use the **show stacking** command to display the current switch stack information. The syntax of the **show stacking** command is as follows:

show stacking {**mode/version**}

Using the optional parameter **mode** displays only the stacking mode of the switches in the switch stack.

Using the optional parameter **version** displays only the stacking firmware version of the switches in the switch stack.

Entering the **show stacking** command with no parameters returns all of the relevant stacking information for all of the switches in the stack:

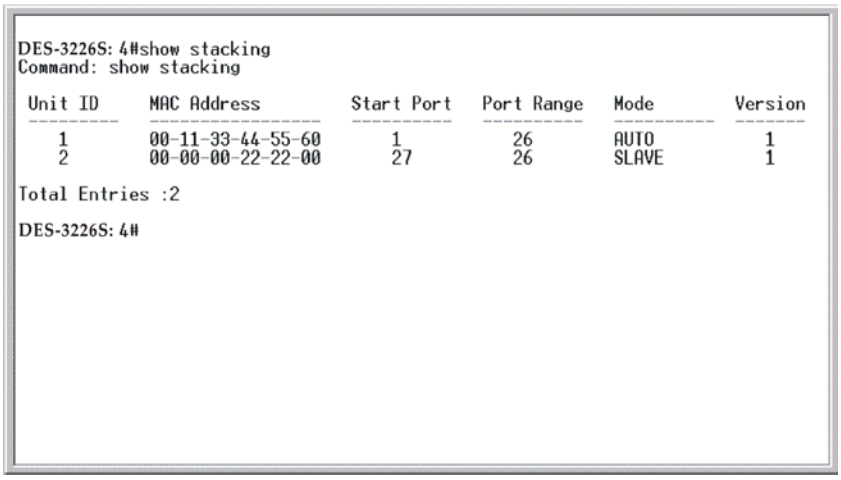


Figure 6 - 13. Console CLI show stack Command

The same switch stack information is displayed in the console as is displayed in the Web-based management agent.

The **config stack** command allows you to configure the switch stack manually.

The syntax of the **config stacking** command is as follows:

config stacking mode
[auto/master/slave/standalone]

One of the parameters **auto/master/slave/standalone** must be entered along with the **config stacking mode** command. These parameters have the following effects:

auto Switches in the stack will be assigned a unit ID sing a comparison of the numerical value of the switch's MAC address. The lowest MAC address in the switch stack will become Unit 1 (the Master Switch), the next highest MAC address

will become Unit 2, and so on. This is the switch's default mode.

master The switch that the management station is connected to (via the switch's serial port) will become Unit 1 – the master switch. This switch will then be used to configure the switch stack.

slave The switch that the management station is connected to (via the switch's serial port) will never become the Master Switch and will always be Unit 2 or higher. If multiple switches in the stack are configured as **slave** switches, their unit numbers are determined by the numerical value of their respective MAC addresses.

standalone This command effectively removes the switch connected to the management station (via the switch's serial port) from the switch stack. The switch will be assigned a Unit number of 1 and cannot be managed as part of the switch stack. When a switch in a switch stack is configured as **standalone**, stacking information is still passed over the stacking link to other switches in the stack.

The following example configures the two switches in a two-switch stack to give the switch with the lowest MAC address a Unit number greater than 1 (configured as a **slave**). The second switch is configured to always have a Unit number of 1 (configured as the **master**):

With the management station's console connected to the serial port of the switch with the lowest MAC address, enter the following command at the prompt:

config stacking mode slave

This will configure the switch with MAC address 00-00-00-22-22-00 to always have a Unit number greater than 1 (as a **slave**).

Now you will have to move the management station's console connection (via the serial port) to the switch with MAC address 00-11-33-44-55-60, and enter the following command:

config stacking mode master

This will configure the switch with MAC address 00-11-33-44-55-60 to always have a Unit number of 1 (as the **master**).

You can then use the **show stacking** command to verify the stacking configuration, as shown below:

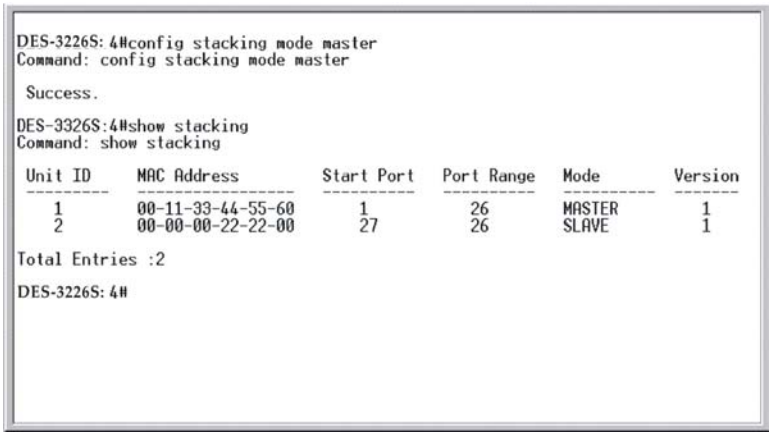


Figure 6 - 14. config stacking Command

Configure Ports

Click the **Port Configurations** link in the **Basic Setup** folder:

For stacked switch installations, it will be necessary to select the Unit (switch) according to its logical position in the stack.

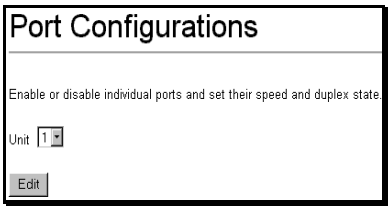


Figure 6 - 15. Choose switch from stack

Click the selection button on the far left that corresponds to the port you want to configure and click the Edit button.

	Port	State	Setting	Connection	Learn
○	1	Enabled	Auto/Disabled	Link Down	Enabled
○	2	Enabled	Auto/Disabled	Link Down	Enabled
○	3	Enabled	Auto/Disabled	100M/Full/None	Enabled
○	4	Enabled	Auto/Disabled	Link Down	Enabled
○	5	Enabled	Auto/Disabled	Link Down	Enabled
○	6	Enabled	Auto/Disabled	Link Down	Enabled
○	7	Enabled	Auto/Disabled	Link Down	Enabled
○	8	Enabled	Auto/Disabled	Link Down	Enabled
○	9	Enabled	Auto/Disabled	Link Down	Enabled
○	10	Enabled	Auto/Disabled	Link Down	Enabled
○	11	Enabled	Auto/Disabled	Link Down	Enabled
○	12	Enabled	Auto/Disabled	Link Down	Enabled
○	13	Enabled	Auto/Disabled	Link Down	Enabled
○	14	Enabled	Auto/Disabled	Link Down	Enabled
○	15	Enabled	Auto/Disabled	Link Down	Enabled
○	16	Enabled	Auto/Disabled	Link Down	Enabled
○	17	Enabled	Auto/Disabled	Link Down	Enabled
○	18	Enabled	Auto/Disabled	Link Down	Enabled
○	19	Enabled	Auto/Disabled	Link Down	Enabled
○	20	Enabled	Auto/Disabled	Link Down	Enabled
○	21	Enabled	Auto/Disabled	Link Down	Enabled
○	22	Enabled	Auto/Disabled	Link Down	Enabled
○	23	Enabled	Auto/Disabled	Link Down	Enabled
○	24	Enabled	Auto/Disabled	Link Down	Enabled
○	25	Enabled	Auto/Disabled	Link Down	Enabled
○	26	Enabled	Auto/Disabled	Link Down	Enabled

Figure 6 - 16. Port Configurations

Click on the port you want to configure on the **Port Configurations** menu and then click the **Edit** button. This will open the following dialog box:

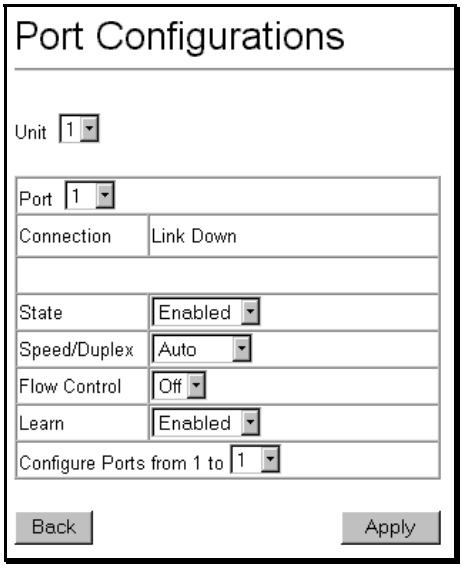


Figure 6 - 17. Port Configurations – Edit

The **Unit** drop-down dialog box allows you to select different switches in a switch stack, if you have the optional stacking module installed and the switches in the stack are properly interconnected.

The **Port** drop-down dialog box allows different ports (on the currently selected Unit) to be selected for configuration.

Use the **State<***Enabled***>** pull-down menu to either enable or disable the selected port.

Use the **Flow Control**<*Off*> pull-down menu to either turn flow control on or off for the selected port.

Use the **Speed/Duplex<***Auto***>** pull-down menu to either select the speed and duplex/half-duplex state of the port. Auto – auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *100M/Full, 100M/Half, 10M/Full,* and *10M/Half*. There is no automatic adjustment of port settings with any option other than *Auto*.

Port Security and MAC Address Learning

A given port's (or a range of port's) dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. The port can be locked by using the **Learn <***Disabled***>** pull-down menu to *Enabled*, and clicking **Apply**.

This is a security feature that prevents unauthorized computers (with source MAC addresses unknown to the switch prior to locking the port (or ports) from connecting to the switch's locked ports and gaining access to the network.

The following fields can be set:

Parameter	Description
State <*Enabled*>	Toggle the **State** <*Enabled*> field to either enable or disable a given port.
Speed/Duplex <*Auto*>	Toggle the **Speed/Duplex** <*Auto*> field to either select the speed and duplex/half-duplex state of the port. Auto – auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *100M/Full*, *100M/Half*, *10M/Full*, and *10M/Half*. There is no automatic adjustment of port settings with any option other than *Auto*.
Flow Control: Auto	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two.
Learn <*Disabled*>	Allows the selected port (or port's) dynamic MAC address learning to be

locked such that new source MAC addresses can not be entered into the MAC address table for the locked port. It can be changed by toggling between *Disabled* and *Enabled*.

Port Security Settings

Click the selection button on the far left that corresponds to the port you want to configure and click the Edit button.

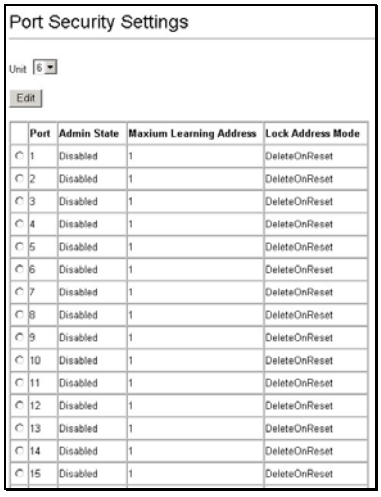


Figure 6 - 18. Configure Port Security

Select the port you want to configure and click Edit. The Port Security Edit menu appears, notice that once this menu is available you may move to any port on any switch in the stack to configure security for that port.

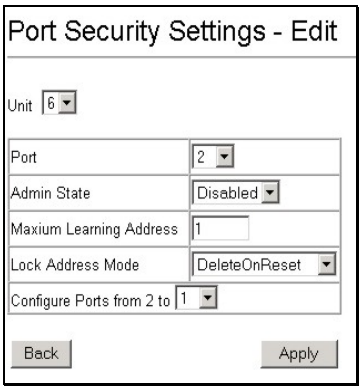


Figure 6 - 19. Port Security Settings

Configure the following parameters for Port Security:

Parameter	Description
Admin State <*Disabled*>	Toggle Admin State to either enable or disable port security for the port.
Max Learning Address <*1* >	Select the maximum number of addresses that may be learned for the port. The port can be restricted to 10 or less MAC addresses that are allowed for dynamically learned MAC addresses in the forwarding table.
Lock Address Mode <*Delete On Reset*>	Select *Delete On Timeout* to clear dynamic entries for the ports on timeout of the Forwarding Data Base (FDB). Specify *Delete On Reset* to delete all FDB entries, including static entries upon system reset or rebooting.
Configure Ports from __ to __	Use this to specify a consecutively numbered group of ports on the switch for configuration.

for configuration.

Traffic Segmentation

The traffic segmentation table is used to limit traffic flow from a single port to other ports on the switch. It cannot be used to segment traffic between switch units in a stack. For this it would be appropriate to use VLANs or a filtering method. This provides an additional tool to direct traffic flow without relying on the Master CPU.

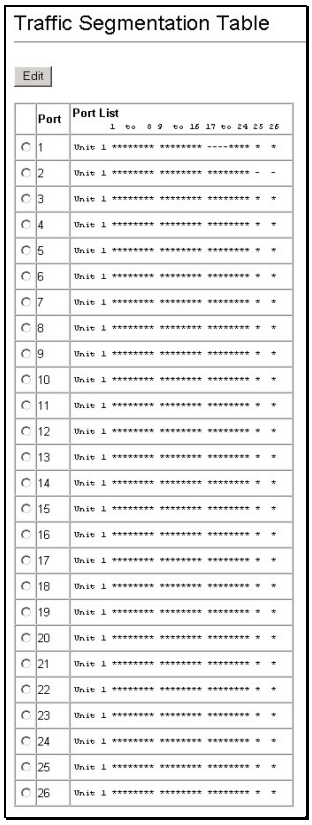


Figure 6 - 20. Traffic Segmentation Table

Click the selection button on the far left that corresponds to the port you want to configure and click the Edit button. This will open the following dialog box:

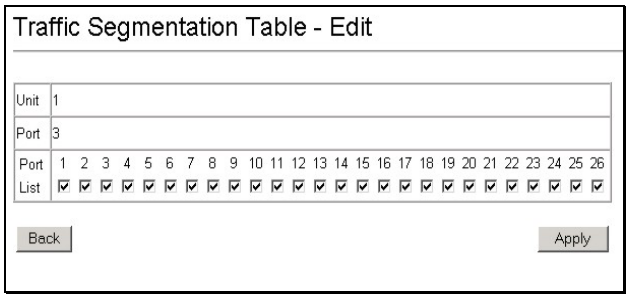


Figure 6 - 21. Traffic Segmentation – Edit

To configure Traffic Segmentation for a port, select the ports from the Port List that are allowed to receive forwarded frames from the port that is being configured. Click the Apply button to add the ports to the forward list.

Serial Port Settings

The **Serial Port Settings** window allows the configuration of the switch's serial port.

Click on the **Serial Port Settings** link from the **Basic Setup** folder.

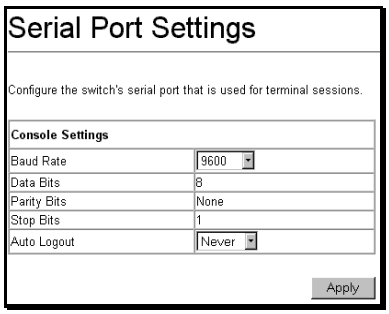


Figure 6 - 22. Serial Port Settings

The following fields can then be set for the serial port:

Parameter	Description

Baud Rate	Set the serial bit rate used to communicate with a management station. The console baud rate is 9600 bits per second.
Data Bits	Displays the number of bits that make up a word when communicating with the management station. The console interface uses 8 data bits.
Stop Bits	Displays the number of bits used to indicate that a word has been completely transmitted. The console interface uses 1 stop bit.
Auto-Logout	This sets the time the interface can be idle before the switch automatically logs-out the user. The options are *2 mins, 5 mins, 10 mins, 15 mins,* or *Never*.

NETWORK MANAGEMENT

The DES-3226S incorporates a flexible SNMP management for the switching environment. SNMP management can be customized o suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

SNMP Settings

The DES-3226S supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The SNMP version used to monitor and control the switch can be specified by the administrator. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the web manager. Workstations on the network that are allowed SNMP privileged access to the switch can be restricted with the Management Station IP Address menu.

SNMP View Table

The SNMP View Table is used to assign views to community strings that define which MIB objects can be accessed by an SNMP manager.

To delete an existing View Table entry, click the selection button on the far left that corresponds to the port you want to configure and click the Delete button. To create a new entry, click the New button, a separate menu will appear.

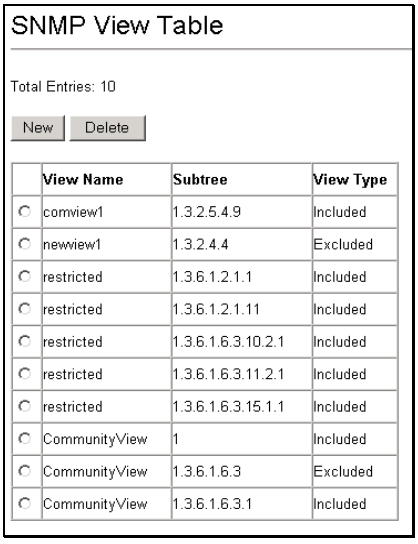


Figure 6 - 23. SNMP View Table

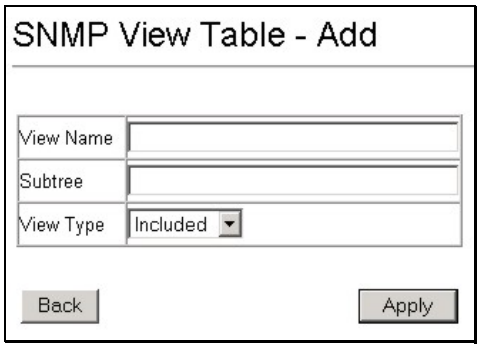


Figure 6 - 24. SNMP View Table – Add New

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select *Included* to include this object in the list of objects that an SNMP manager can access. Select *Excluded* to exclude this object from the list of objects that an SNMP manager can access.

SNMP Group Table

The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous menu.

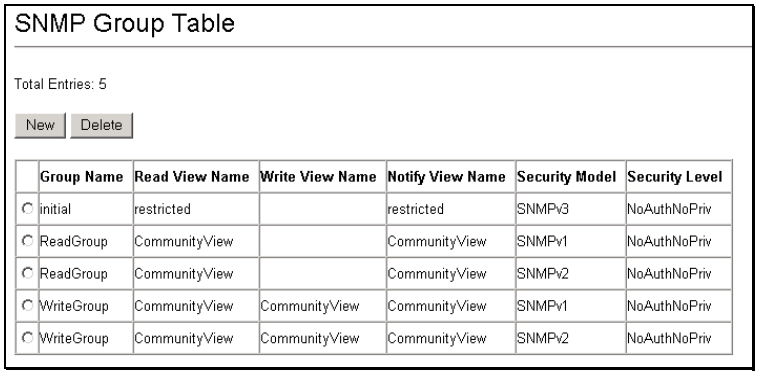


Figure 6 - 25. SNMP Group Table

To delete an existing entry, click the selection button on the far left that corresponds to the port you want to configure and click the Delete button. To create a new entry, click the New button, a separate menu will appear.

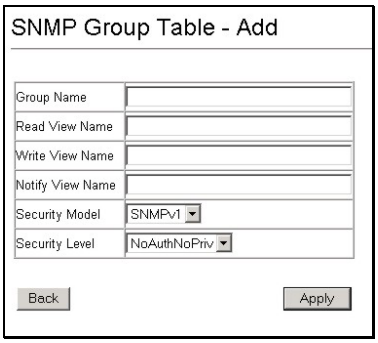


Figure 6 - 26.SNMP Group – Add New

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the switch's SNMP agent.
Security Model	Use the pull-down menu to select the SNMP version. Select one of the following: *SNMPv1* – Specifies that SNMP version 1 will be used. *SNMPv2* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.

	USM – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	Use the pull-down menu to select the SNMP version: *NoAuthNoPriv* – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager. *AuthNoPriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager. *AuthPriv* – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.

SNMP Community Table

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the switch. One or more of the following characteristics can be associated with the community string:

An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the switch's SNMP agent.

An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community.

Read/write or read-only level permission for the MIB objects accessible to the SNMP community

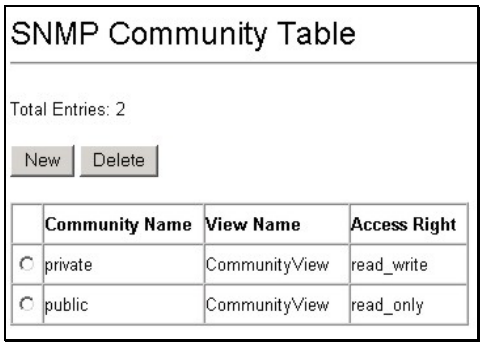


Figure 6 - 27. SNMP Community Table

To delete an existing entry, click the selection button on the far left that corresponds to the port you want to configure and click the Delete button. To create a new entry, click the New button, a separate menu will appear. Configure the parameters as desired and click the Apply button to add the new string to the SNMP Community Table.

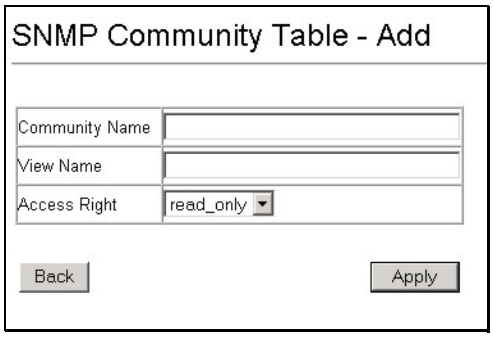


Figure 6 - 28. SNMP Community Table – Add New

Configure the following for the new SNMP Community entry:

Parameter	Description
Community Name	Type an alphanumeric string of up to 33 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch. The view name must exist in the SNMP View Table.
Access Right	Use the pull-down menu to select the access right: read_only – Specifies that SNMP community members using the community string created with this command can only read the contents

	of the MIBs on the switch. read_write – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the switch.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the switch.

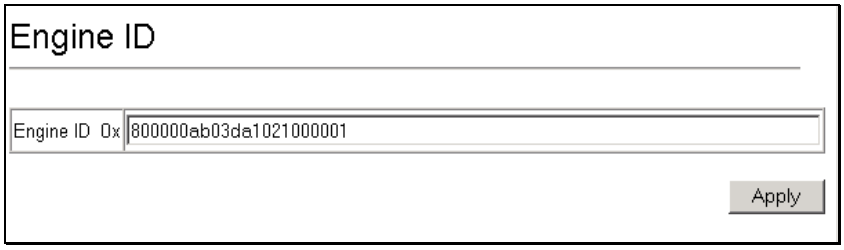


Figure 6 - 29. Engine ID

To change the Engine ID, type the new Engine ID in the space provided and click the Apply button.

SNMP Host Table

Use the SNMP Host Table to set up trap recipients.

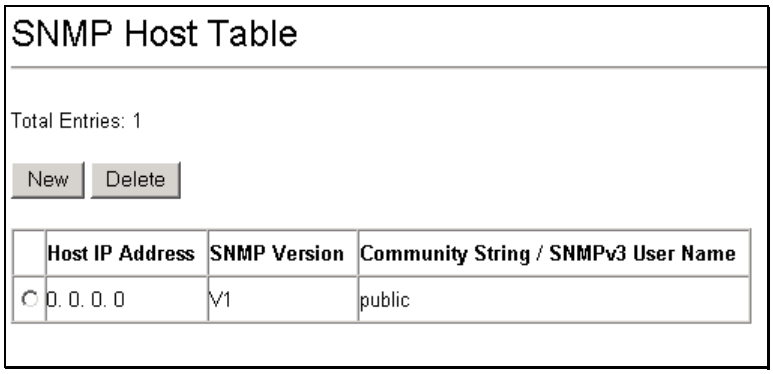


Figure 6 - 30. SNMP Host Table

To delete an existing entry, click the selection button on the far left that corresponds to the port you want to configure and click the Delete button. To create a new entry, click the New button, a separate menu will appear.

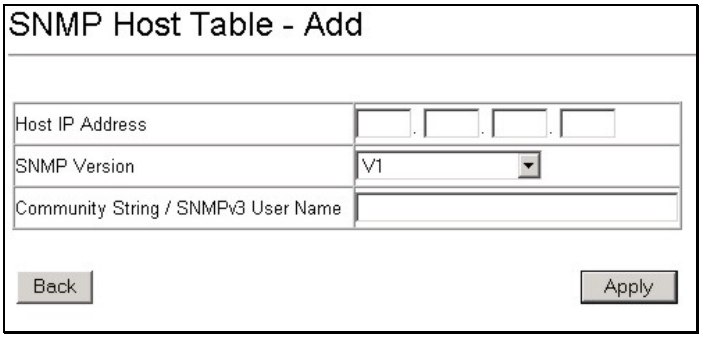


Figure 6 - 31. SNMP Host Table – Add New

Parameter	Description
IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the switch.
SNMP Version	From the pull-down menu select: V1 – To specifies that SNMP version 1 will be used. V2 – To specify that SNMP version 2 will be used. V3 – To specify that the SNMP version 3 will be used.
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

SNMP User Table

Use the SNMP User Table to create a new SNMP user and add the user to an existing SNMP group or to a newly created group.

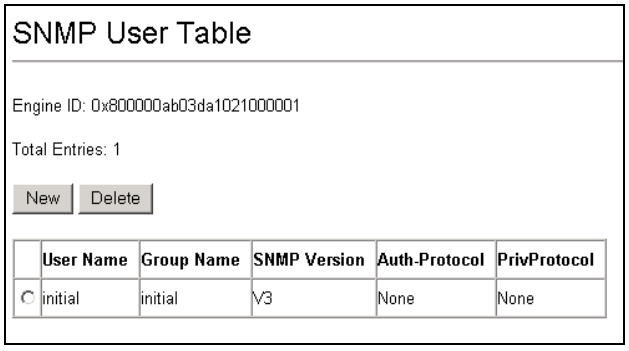


Figure 6 - 32. SNMP User Table

To delete an existing entry, click the selection button on the far left that corresponds to the port you want to configure and click the Delete button. To create a new entry, click the New button, a separate menu will appear.

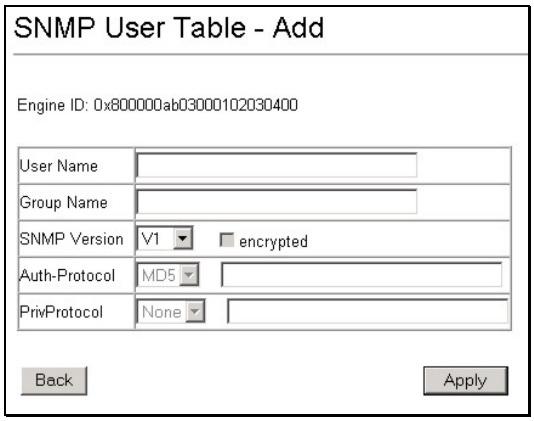


Figure 6 - 33. SNMP User Table – Add New

Parameter	Description
User Name	Type in the new SNMP V3 user name or community string for V1 or V2. This can be any alphanumeric name of up to 32 characters that will identify the new SNMP user.
Group Name	Type in the new SNMP V3 group name. Again, this can be any alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.

SNMP Version	From the pull-down menu select: V1 – To specifies that SNMP version 1 will be used. V2 – To specify that SNMP version 2 will be used. V3 – To specify that the SNMP version 3 will be used.
If Encryption (V3 only) is checked configure also:	
Auth-Protocol	In the Space provided, type an alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host. From the pull-down menu select: **MD5** – To specify that the HMAC-MD5-96 authentication level will be used. **SHA** – To specify that the HMAC-SHA-96 authentication level will be used.
If Encryption (V3 only) is checked configure also:	
Priv-Protocol	In the Space provided, type an alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.

ADVANCED SETUP

Configuring VLANs

To create a new 802.1Q VLAN:

The VLAN menu adds an entry to edit the VLAN definitions and to configure the port settings for IEEE 802.1Q VLAN support. Go to the **Advanced Setup** folder, select **VLAN Configurations**, and click the **802.1Q VLANs** link to open the following dialog box:

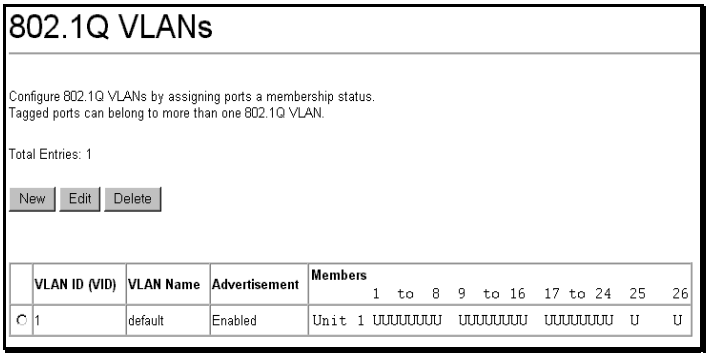


Figure 6 - 34. 802.1Q VLANs

To delete an existing 802.1Q VLAN, click the corresponding click-box to the left of the VLAN you want to delete from the switch and then click the **Delete** button.

To create a new 802.1Q VLAN, click the New button:

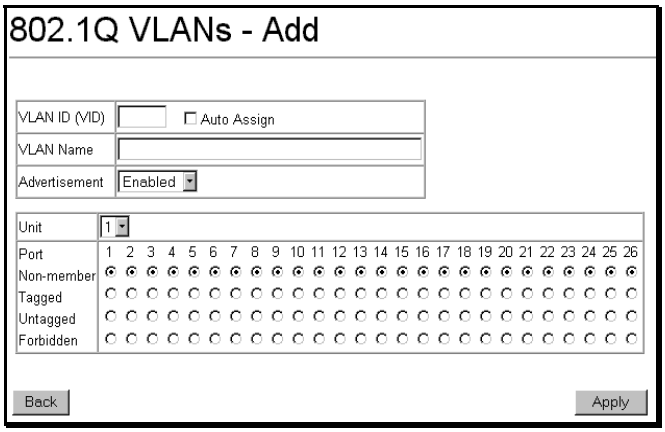


Figure 6 - 35. 802.1Q Static VLANs Entry Settings – Add

To edit an existing 802.1Q VLAN, click the corresponding click-box and then click the Edit icon to open the following dialog box:

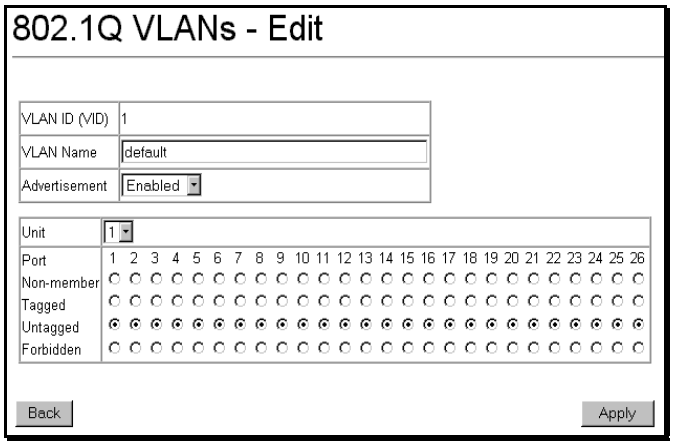


Figure 6 - 36. 802.1Q Static VLANs Entry Settings – Edit

The following fields can then be set in either the **Add** or **Edit** dialog boxes:

Parameter	Description
VLAN ID (VID)	Allows the entry of a VLAN ID in the **Add** dialog box, or displays the VLAN ID of an existing VLAN in the **Edit** dialog box. VLANs can be identified by either the VID or the VLAN name. The **Auto Assign** click box will instruct the switch to assign VLAN IDs – in ascending numerical order starting with 1 – to each VLAN as it is created.
VLAN Name	Allows the entry of a name for the new VLAN in the **Add** dialog box, or for editing the VLAN name in the **Edit** dialog box.
Advertisement	Advertising can be enabled or disabled using this pull-down menu. Advertising allows members to join this VLAN through GVRP.
Port	Allows an individual port to be specified as member of a VLAN.
Tagged/Untagged	Allows an individual port to be specified as Tagging. A Check in the **Tagged** field specifies the port as a Tagging member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the VID (VLAN Identifier – see below). When a tagged packet exits the port, the packet header is unchanged.

Untagged	Allows an individual port to be specified as **Untagged.** When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.
Egress	Egress Member - specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
Forbidden	Forbidden Non-Member - specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

The **Port VLAN ID (PVID)** dialog box, shown below, allows you to determine whether the switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (**GVRP**) enabled switches. In addition, **Ingress Checking** can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port.

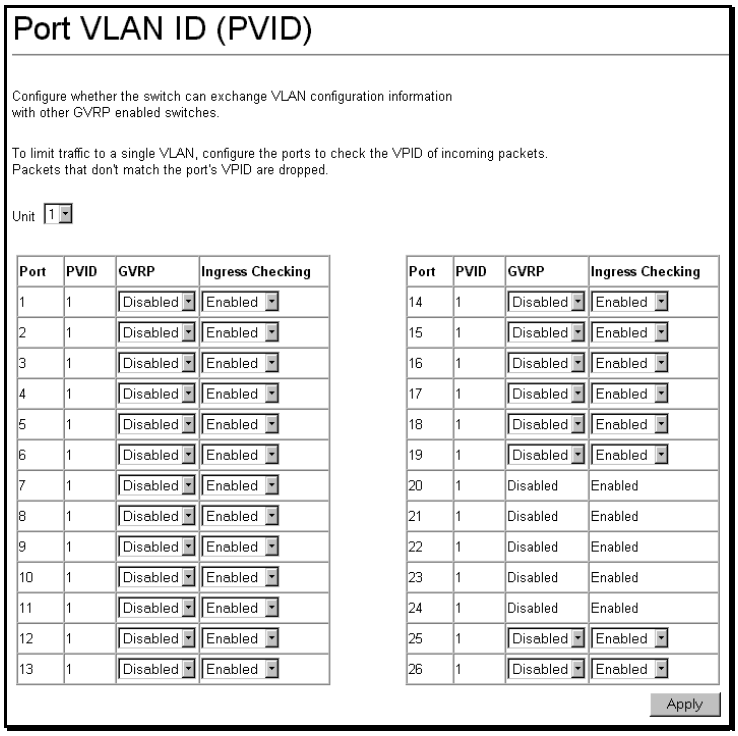


Figure 6 - 37. Port VLAN ID (PVID)

The following fields can be set:

Parameter	Description
PVID	A Port VLAN Identifier is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the Edit 802.1Q VLANs menu above.
GVRP <*Disabled*>	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN.
Ingress Checking <*Disabled*>	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables Ingress filtering.

To enable or disable GVRP, globally, on the switch:

Go to the **VLAN Configurations** link and click on the **Switch GVRP** link:

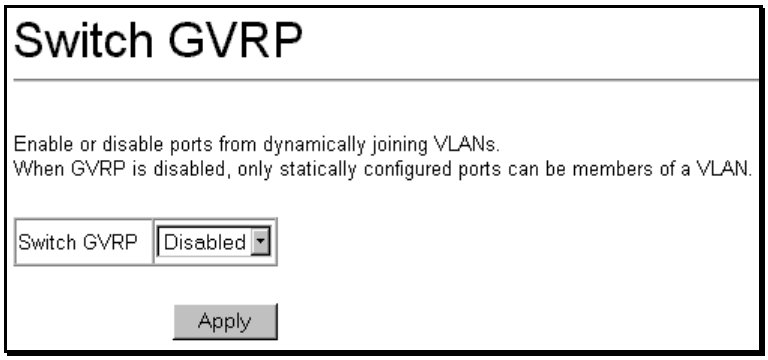


Figure 6 - 38. – Switch GVRP

Parameter	Description
GVRP <*disabled*>	Group VLAN Registration Protocol (GVRP) – this enables and disables GVRP on the switch without changing the port GVRP settings.

Configure QOS (Quality of Service)

The DES-3226S switch supports 802.1p priority queuing. The switch has 4 priority queues. These priority queues are numbered from 0 — the lowest priority queue — to 3 — the highest priority queue. The eight priority queues specified in IEEE 802.1p (Q0 to Q7) are mapped to the switch's priority queues as follows:

Q1 and Q2 are assigned to the switch's Q0 queue.

Q0 and Q3 are assigned to the switch's Q1 queue.

Q4 and Q5 are assigned to the switch's Q2 queue.

Q6 and Q7 are assigned to the switch's Q3 queue.

The switch's four priority queues are emptied in a round-robin fashion—beginning with the highest priority queue, and proceeding to the lowest priority queue before returning to the highest priority queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Only when these queues are empty, are packets of lower priority transmitted.

The weighted-priority based scheduling alleviates the main disadvantage of strict priority-based scheduling – in that lower priority queues get starved of bandwidth – by providing a minimum bandwidth to all queues for transmission. This is accomplished by configuring the maximum number of packets allowed to be transmitted from a given priority queue and the maximum amount of time a given priority queue will have to wait before being allowed to transmit its accumulated packets. This establishes a Class of Service (CoS) for each of the switch's four hardware priority queues.

The possible range for maximum packets is: 0 to 255 packets.

The possible range for maximum latency is: 0 to 255 (in increments of 16 microseconds each).

Remember that the DES-3226S has four priority queues (and thus four Classes of Service) for each port on the switch.

Configuring QOS Output Scheduling

Click the **Configure QOS** link on the **Advanced Setup** menu, and the click on the **QOS Output Scheduling** link:

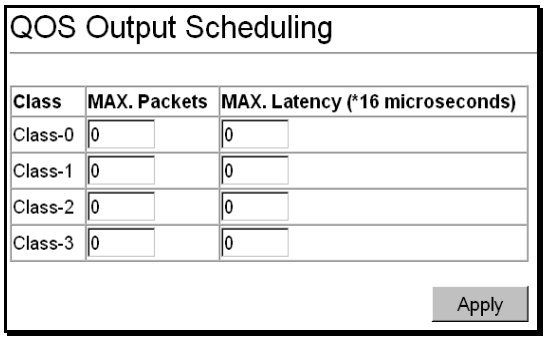


Figure 6 - 39. QOS Output Scheduling

The MAX. Packets field specifies the number of packets that a queue will transmit before surrendering the transmit buffer to the next lower priority queue in a round-robin fashion.

The MAX. Latency field specifies the maximum amount of time—in multiples of 16 microseconds—that a queue will have to wait before being given access to the transmit buffer. The MAX. Latency is a priority queue timer. When it expires, it overrides the round-robin and gives the priority queue that it was set for access to the transmit buffer.

There is a small amount of additional latency introduced because the priority queue that is transmitting at the time the MAX. Latency time

expires will finish transmitting its current packet before giving up the transmit buffer.

Configuring Default Priority

The switch allows the assignment of a default 802.1p priority to each port on the switch.

Click on the **Default Priority** link:

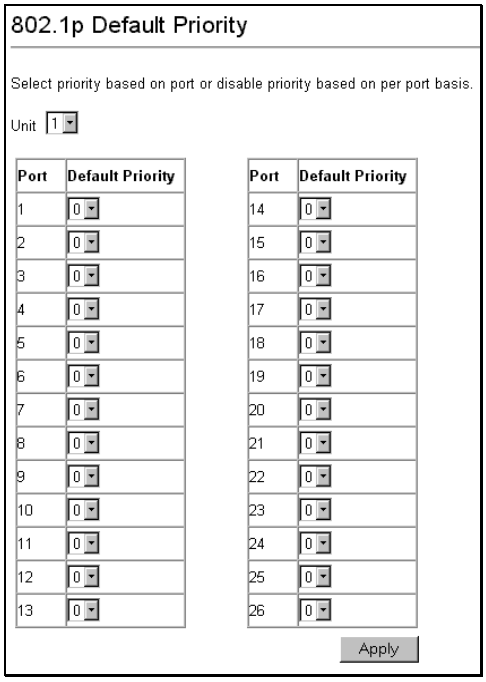


Figure 6 - 40. Priority Based on Port

This window allows you to assign a default 802.1p priority to any given port on the switch. The priority queues are numbered from 0 – the lowest priority – to 7 – the highest priority.

Configuring 802.1p User Priority

The DES-3226S allows the assignment of a User Priority to each of the 802.1p priorities.

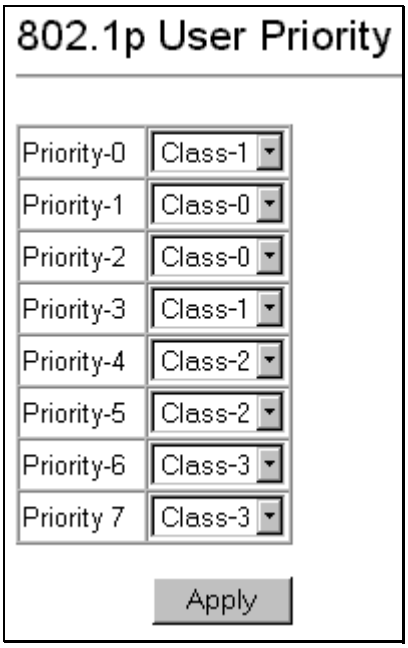


Figure 6 - 41. QOS Class of Traffic

Once you have assigned a maximum number of packets and a maximum latency to a given Class of Service on the switch, you can then assign this Class to each of the 8 levels of 802.1p priorities.

Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data bit rates for any port.

To change the maximum allowed bandwidth for a given port:

In the Bandwidth Control Table, click the selection button in the far left column that corresponds to the port you want to configure and click the Edit button. A new dialog box used to edit bandwidth settings opens.

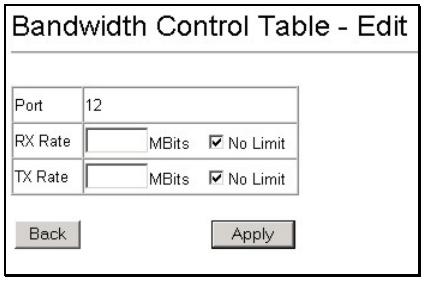


Figure 6 - 42. Edit Port Bandwidth

To limit either the Rx or Tx rates, deselect the No Limit check box and type the desired rate. Rates can be expressed using whole numbers up to the maximum available rate for the port.

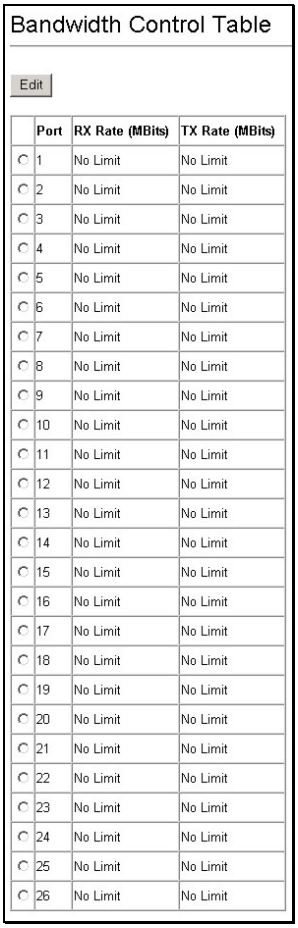


Figure 6 - 43. Bandwidth Control Table

Port Mirroring

To configure a port for port mirroring:

Click the **Mirroring** link and then the **Target Port Selection** link:

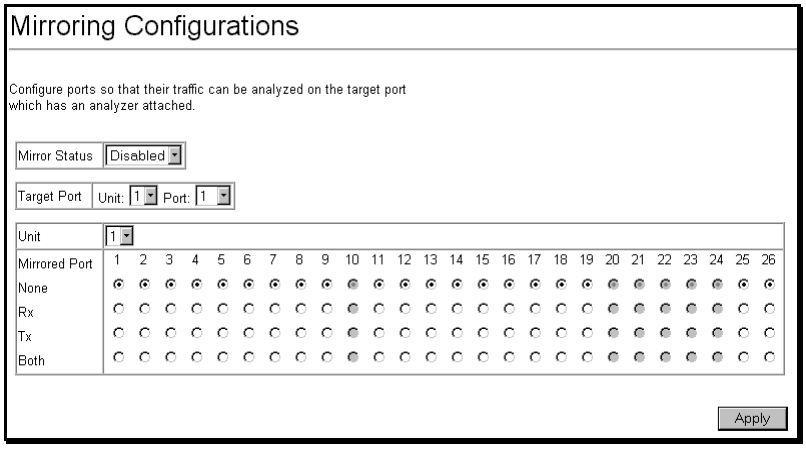


Figure 6 - 44. Target Port Selection

The target port is the port where information will be duplicated and sent for capture and network analysis. This is the port where a network analyzer would be attached to capture packets duplicated from the source port.

Up to 25 entries can be made to the port mirroring table, but it should be noted that a faster port (a 1000 Mbps Gigabit Ethernet port, for example) should not be mirrored to a slower port (one of the 24 100 Mbps Fast Ethernet port), because many packets will be dropped.

The following fields can be set:

Parameter	Description
Source Port	Allows the entry of the port number of the port to be mirrored. This port is the source of the packets to be duplicated and forwarded to the Target port.
Direction <*Ingress*>	This field can be toggled between *Either*, *Ingress* and *Egress*. *Ingress* mirrors only received packets, while *Egress* mirrors only transmitted packets.

Forwarding

MAC Address Aging Time

The **MAC Address Aging Time** specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between **300** and **1,000,000** seconds.

To configure the MAC Address Aging Time, click on the Forwarding folder and then the MAC Forwarding folder, then click on the MAC Address Aging Time link:

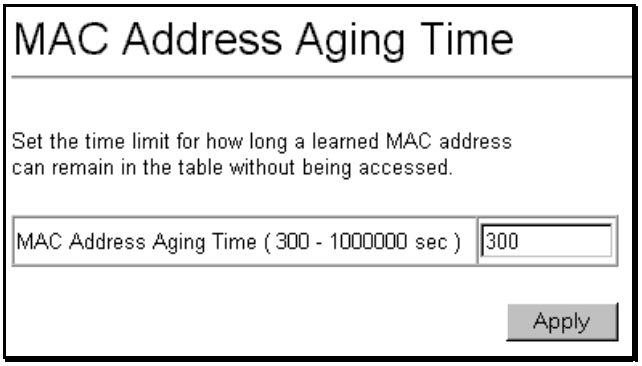


Figure 6 - 45. MAC Address Aging Time

Unicast MAC Address Forwarding

MAC addresses can be statically entered into the switch's MAC Address Forwarding Table. These addresses will never age out.

To enter a MAC address into the switch's forwarding table, click on the Forwarding folder and then the MAC

Forwarding folder and then click the Unicast MAC Address Setting:

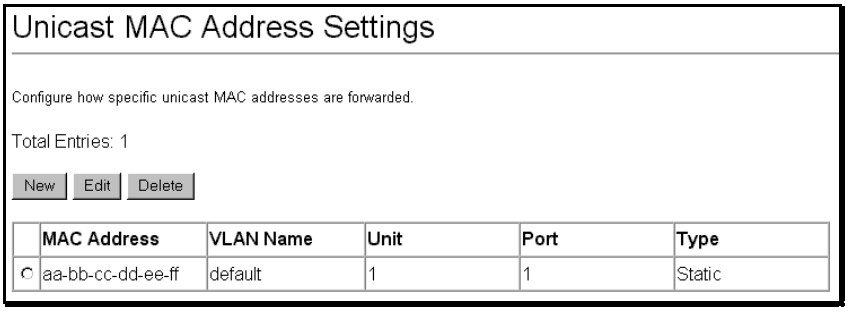


Figure 6 - 46. Unicast MAC Address Settings

To add a new MAC address to the MAC Address Forwarding Table, click the New button:

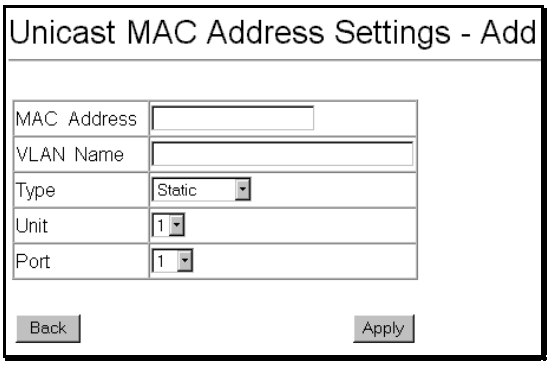


Figure 6 - 47. Unicast MAC Address Settings – Add

To edit an existing entry in the MAC address in the MAC Address Forwarding Table, click the Edit button:

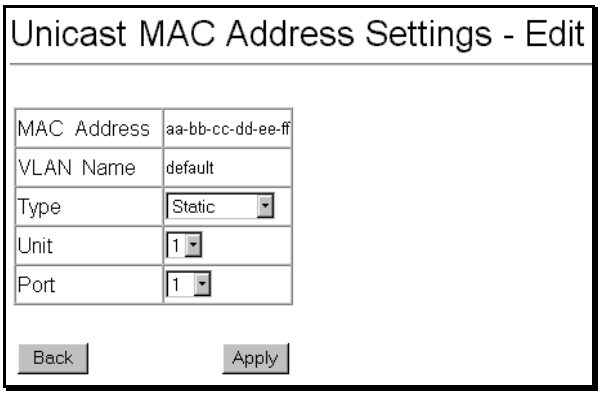


Figure 6 - 48. Unicast MAC Address Settings – Edit

The following fields can be set:

Parameter	Description
MAC Address	Allows the entry of the MAC address of an end station that will be entered into the switch's static forwarding table when adding a new entry. Displays the currently selected MAC address when editing.
VLAN Name	Allows the entry of the VLAN Name of the VLAN the MAC address below is a member of – when editing. Displays the VLAN the currently selected MAC address is a member of – when editing an existing entry.
Unit	Allows the selection of a given switch from a switch stack – if you have the optional stacking module installed and have properly interconnected the

	switches in a switch stack.
Port	Allows the entry of the port number on which the MAC address entered above resides.

Multicast MAC Address Forwarding

Multicast MAC addresses can be statically entered into the switch's MAC Address Forwarding Table. These addresses will never age out.

To enter a Multicast MAC address into the switch's forwarding table, click on the Forwarding folder and then the MAC Forwarding folder and then click on the Multicast MAC Address Settings link:

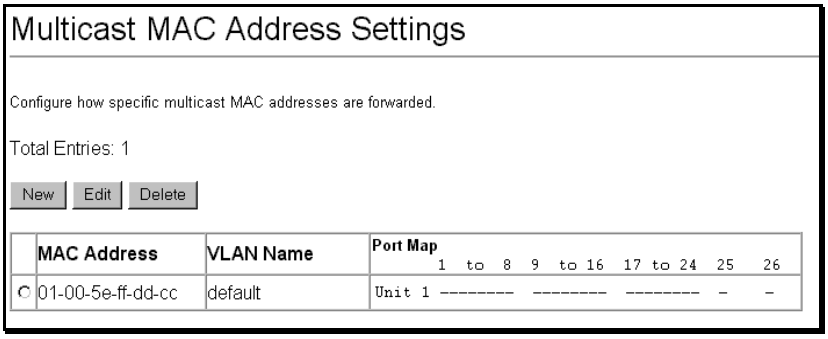


Figure 6 - 49. Multicast MAC Address Settings

To add a new multicast MAC address to the switch's forwarding table, click the New button:

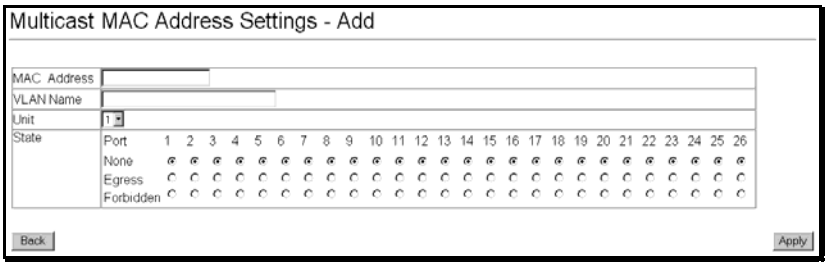


Figure 6 - 50. Multicast MAC Address Settings – Add

To edit an existing entry to the switch's forwarding table, click the entry's corresponding click-box and then click the edit button:

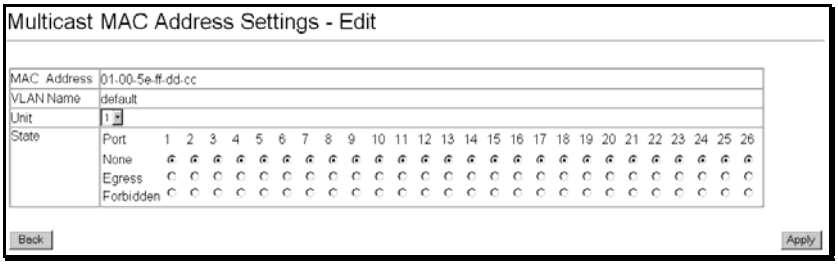


Figure 6 - 51. Multicast MAC Address Settings – Edit

The following fields can be set:

Parameter	Description
MAC Address:[ ]	Allows the entry of the MAC address of an end station that will be entered into the switch's static forwarding table.
VLAN Name	Allows the entry of the VLAN name of the VLAN the MAC address below is a member of – when adding a new entry to the table. Displays the VLAN name of the VLAN the MAC address is a member of – when editing an existing entry.
Port: [ ]	Allows the entry of the port number on which the MAC address entered above resides.
None	Specifies the port as being none.
Egress	Specifies the port as being a source of multicast packets originating from the MAC address specified above.
Forbidden	Forbidden Non-Member - specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Broadcast/Multicast Storm Control

Broadcast and Multicast storms consist of broadcast or multicast packets that flood and/or are looped on a network causing noticeable performance degradation and, in extreme cases, network failure.

The DES-3226S allows some control over broadcast/multicast storms by setting thresholds on the number of broadcast/multicast packets received (in thousands of packets per second or Kpps), and then following a user-specified course of action when this threshold is exceeded.

To configure Broadcast/Multicast storm control:

Click on the **Forwarding** folder, and then on the **MAC Forwarding** folder, and finally on the **Broadcast/Multicast Storm Control** link:

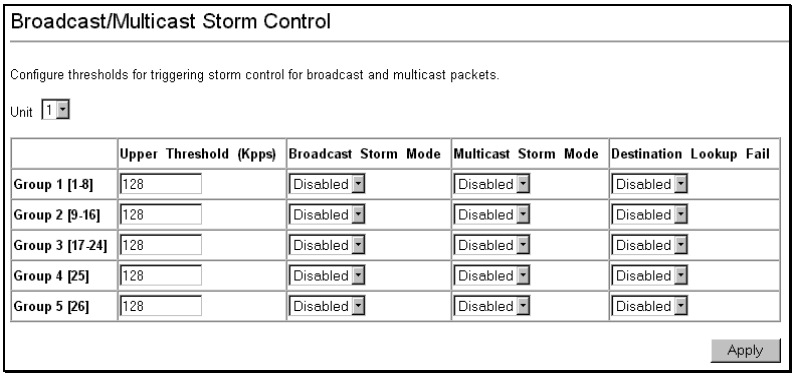


Figure 6 - 52. Broadcast/Multicast Storm Control

Broadcast/Multicast storm control is applied to groups of ports on the DES-3226S. **Group 1** contains ports 1 through 8. **Group 2** contains ports 9 through 16. **Group 3** contains ports 17 through 24. **Group 4** and **Group 5** contain the ports on the optional plug-in module.

The **Upper Threshold (Kpps)** sets the rate of broadcast or multicast packets received on any of the ports in the corresponding port group that will trigger the action to be taken by the switch, as detailed below. A range of thousands of packets received per second (Kpps) between 0 and 255 can be specified.

When any one of the ports contained within a given port group receives more broadcast or multicast packets per second than is specified in the **Upper Threshold (Kpps)** field, the switch will take the actions specified in the **Broadcast Storm Mode, Multicast Storm Mode,** and the **Destination Lookup Fail** pull-down menus.

The **Broadcast Storm Mode** is **Enabled** or **Disabled** using the pull-down menu for the corresponding port group. When the **Broadcast Storm Mode** is enabled, and a port contained within the corresponding port group receives more broadcast packets than specified in the **Upper Threshold (Kpps)** field, the switch will drop all broadcast packets received by any port in the port group until the rate of broadcast packets received by the port group falls.

The **Multicast Storm Mode** is **Enabled** or **Disabled** using the pull-down menu for the corresponding port group. When the **Multicast Storm Mode** is enabled, and a port contained within the corresponding port group receives more multicast packets than specified in the **Upper Threshold (Kpps)** field, the switch will drop all multicast packets received by any port in the port group until the rate of multicast packets received by the port group falls.

The **Destination Lookup Fail** is **Enabled** or **Disabled** using the pull-down menu for the corresponding port group. When the **Destination Lookup Fail** is enabled, and a port contained within the corresponding port group receives more destination lookup failed packets than specified in the **Upper Threshold (Kpps)** field, the switch will drop all destination lookup failed packets received by any port in the port group until the rate of

destination lookup failed packets received by the port group falls.

Spanning Tree

The switch supports 802.1d STP and 802.1w Rapid STP. The spanning tree commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

STP Switch Settings

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

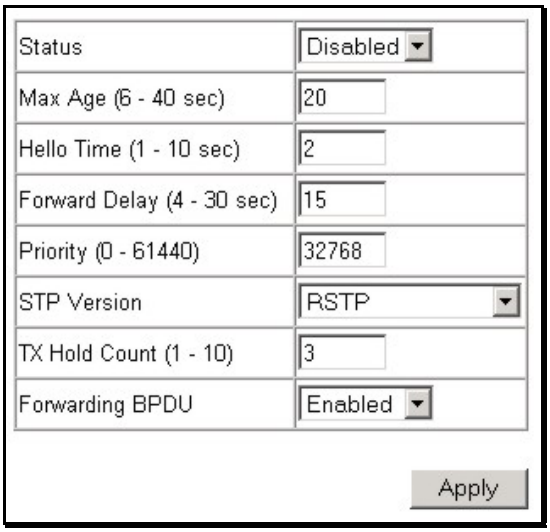


Figure 6 - 53. STP Switch Settings

Configure the following parameters and click the Apply button to implement them:

Parameter	Description
Status <*Disabled*>	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. This will enable or disable the Spanning Tree Protocol (STP), globally, for the switch.
Max Age: (6 - 40 sec) <*20* >	The Max. Age can be set from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.
Hello Time: (1 - 10 sec) < *2* >	The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge.
Forward Delay: (4 - 30 sec) <*15* >	The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.
Priority: (0 - 61440) <*32768*>	A Priority for the switch can be set from 0 to 61440. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be

	elected as the root switch.
STP Version <*RSTP* >	Choose RSTP (default) or STP Compatibility. Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment.
Tx Hold Count <*3* >	This is the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. Default value = 3.
Forwarding BPDU <*Enabled* >	This can enabled or disabled. When it is enabled it allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled.

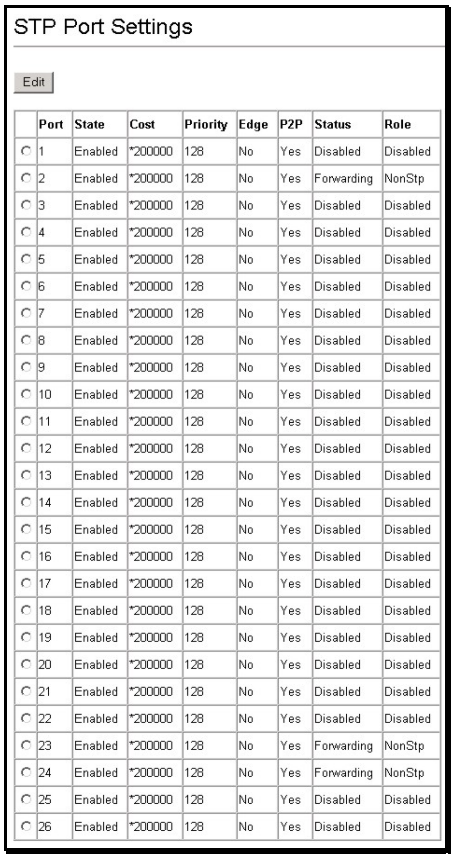
Note: the Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Observe the following formulas when setting the above parameters:

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

STP Port Settings

For stacked switch installations, first select the Unit to be configured.


STP Port Settings

Edit

	Port	State	Cost	Priority	Edge	P2P	Status	Role
○	1	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	2	Enabled	*200000	128	No	Yes	Forwarding	NonStp
○	3	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	4	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	5	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	6	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	7	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	8	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	9	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	10	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	11	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	12	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	13	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	14	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	15	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	16	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	17	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	18	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	19	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	20	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	21	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	22	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	23	Enabled	*200000	128	No	Yes	Forwarding	NonStp
○	24	Enabled	*200000	128	No	Yes	Forwarding	NonStp
○	25	Enabled	*200000	128	No	Yes	Disabled	Disabled
○	26	Enabled	*200000	128	No	Yes	Disabled	Disabled

Figure 6 - 54. STP Port Settings

To change STP settings for a port or a group of ports on the same switch, select the first (lowest numbered) port from the list and click the Edit button, a separate menu will appear.

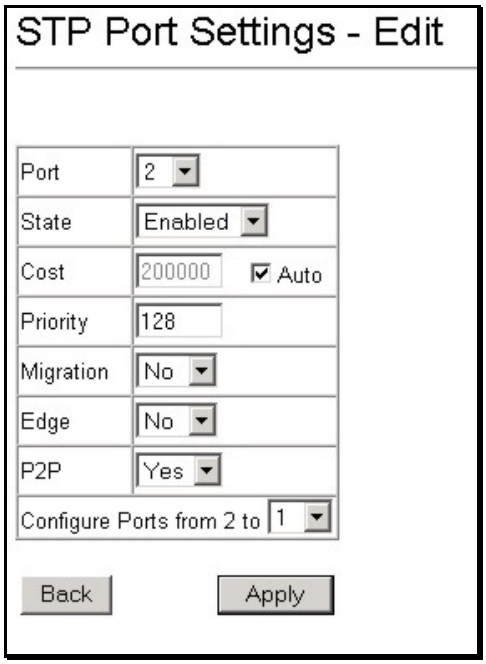


Figure 6 - 55. Edit STP Port Settings

In addition to setting Spanning Tree parameters for use on the switch level, the switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected on the basis of port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The following fields can be set:

Parameter	Description
Cost	A Port Cost can be set from *1* to *200000000*. The lower the number, the greater the probability the port will be chosen to forward packets. Default port cost: 100Mbps port = 200000 Gigabit ports = 20000
Priority <*128*>	A Port Priority can be from *0* to *240*. The lower the number, the greater the probability the port will be chosen as the Root Port.
Migration <*No*>	Select Yes or No. Choosing Yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion

	of the segment.
Edge <*No*>	Select True or False. Choosing true designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. False indicates the port does not have edge port status.
P2P <*Yes*>	Select True or False. Choosing true indicates a point-to-point (p2p) shared link. These are similar to edge ports however they are restricted in that a p2p port must operate in full-duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP.
Configure Ports from __ to __	A consecutive groups of ports may be configured starting with the selected port.

MAC Notification

MAC address notification is used to monitor MAC addresses learned and entered into the forwarding database.

Global Settings

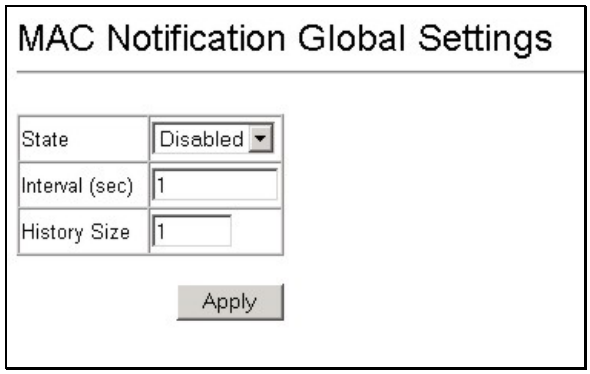


Figure 6 - 56. MAC Notification Global Settings

Configure the following MAC notification global settings:

Parameter	Description
State	Enable or Disable MAC notification switch wide form the pull-down menu.
Interval	This is the time in seconds between notifications.
History Size	This is maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

MAC Notification Port Settings

Enable or disable MAC notification for ports with the menu below.

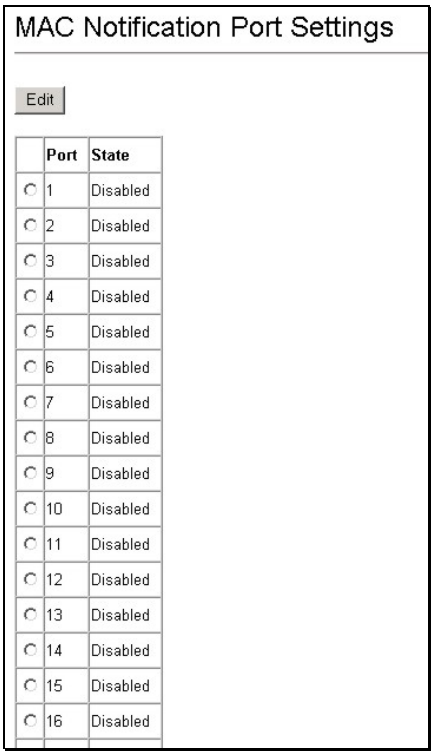


Figure 6 - 57. MAC Notification Port Settings

To change MAC Notification settings for a port or a group of ports on the same switch, select the first (lowest numbered) port from the list and click the Edit button, a separate menu will appear.

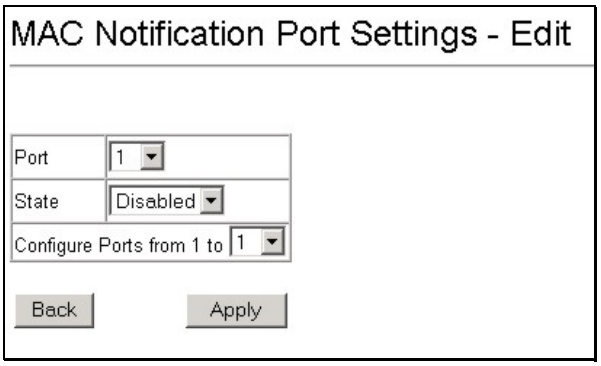


Figure 6 - 58. MAC Notification Port Settings - Edit

Configure the following MAC notification global settings:

Parameter	Description
Port	Select the port or lowest number of the group of ports being configured.
State	Enable or Disable MAC notification for the port from the pull-down menu.
Configure Ports from __ to __	A consecutive groups of ports may be configured starting with the selected port.

Link Aggregation

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

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

The switch allows the creation of up to 6 link aggregation groups, each group consisting of up of up to 8 links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the two (optional) Gigabit ports – which can only belong to a single link aggregation group. A link aggregation group may not cross an 8-port boundary, starting with port 1 (a group may not contain ports 8 and 9, for example) and all of the ports in the group must be members of the same VLAN. Further, the aggregated links must all be of the same speed and should be configured as full-duplex.

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

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

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the

calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the switch, STP will block one entire group – in the same way STP will block a single port that has a redundant link.

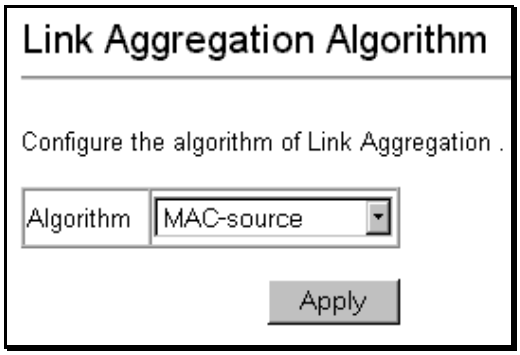


Figure 6 - 59. Link Aggregation Algorithm – Selection

Mac_source – Indicates that the switch should examine the MAC source address.

Mac_destination – Indicates that the switch should examine the MAC destination address.

Mac_source_dest – Indicates that the switch should examine the MAC source and destination addresses.

IP_source – Indicates that the switch should examine the IP source address.

IP_destination – Indicates that the switch should examine the IP destination address.

IP_source_dest – Indicates that the switch should examine the IP source and destination addresses.

To configure a link aggregation group, click on the Link Aggregation link from the Advanced Setup folder:

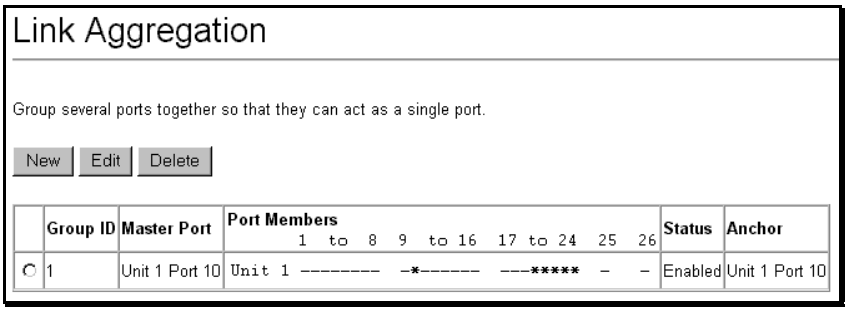


Figure 6 - 60. Link Aggregation

To add a new multicast MAC address to the switch's forwarding table, click the New button:

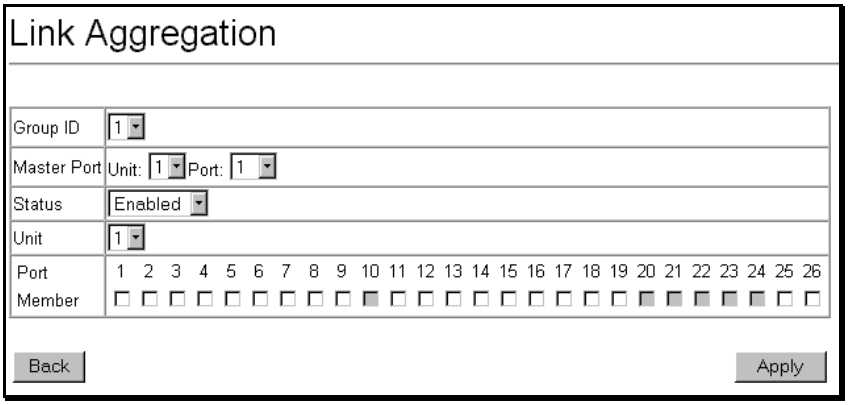


Figure 6 - 61. Link Aggregation – New

To edit an existing entry to the switch's forwarding table, click the entry's corresponding click-box and then click the edit button:

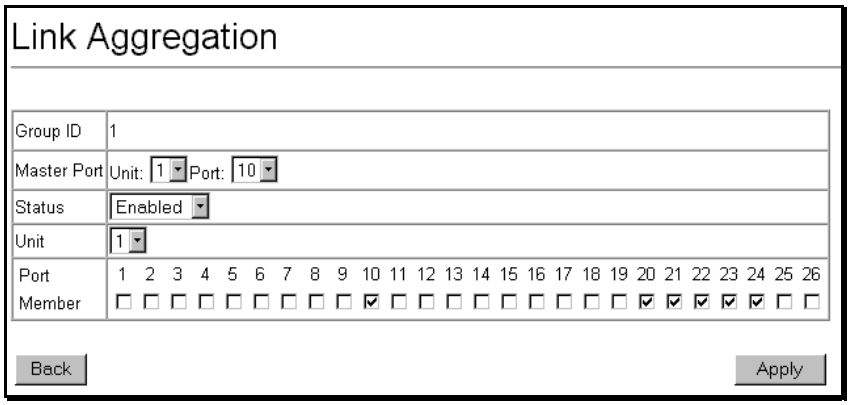


Figure 6 - 62. Link Aggregation – Edit

The following fields can be set:

Parameter	Description
Group ID	Allows the entry of a number used to identify the link aggregation group – when adding a new group. Displays the Group ID of the currently selected link aggregation group – when editing and existing entry.
Master Port <*1*>	The Master port of link aggregation group.
Unit	Allows the selection of a particular switch in a switch stack, if you have the optional stacking module installed and have properly interconnected the switches in the switch stack.

Port Member	Allows the specification of the ports that will make up the link aggregation group.
State <*Disabled*>	This field can be toggled between *Enabled* and *Disabled*. This is used to turn a link aggregation group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup link aggregation group that is not under automatic control.

802.1X Configuration

The DES-3226S implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

IEEE 802.1X operation must be enabled on the switch before it will function. This is done using the 802.1 State menu (see the end of 802.1 Configuration section). 802.1X settings can be configured before it is enabled switch wide.

802.1X Port Settings

Existing 802.1X port settings are displayed and can be con figured using the menu below.

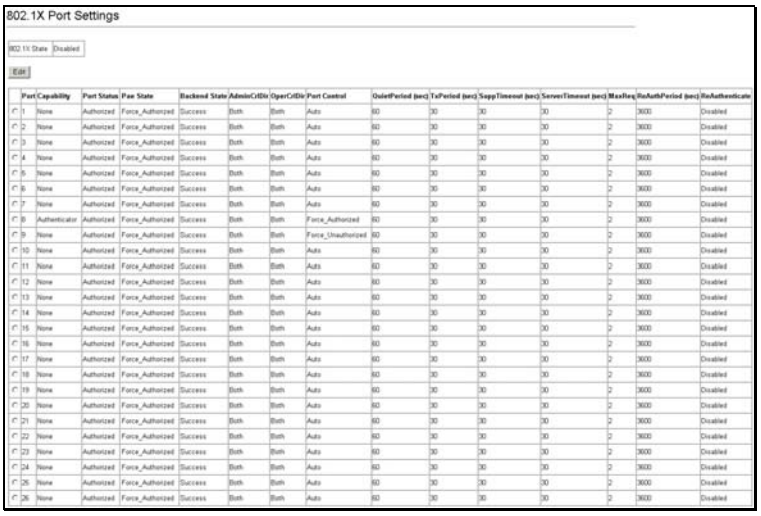


Figure 6 - 63. 802.1X Port Settings

Click the selection button on the far left that corresponds to the port you want to configure and click the Edit button, a separate menu will appear.

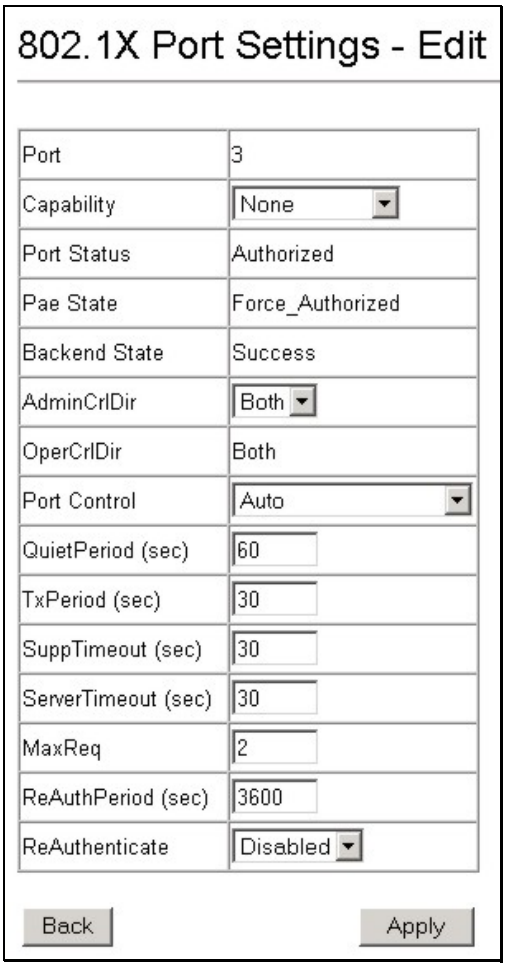


Figure 6 - 64. 802.1X Port Settings – Edit

Configure the following 802.1x port settings:

Parameter	Description
Port	Port being configured for 802.1x settings.
Capability	Two role choices can be selected: Authenticator – A user must pass the authentication process to gain access to the network. None – The port is not controlled by the 802.1x functions.
Port status	Lists the current status of port, Authorized or Unauthorized.
PAE State	Displays the administrative control over the port's authorization status. Force Authorized forces the Authenticator of the port to become Authorized. Force Unauthorized forces the port to become Unauthorized.
Backend State	Shows the current state of the Backend Authenticator.
AdminCtlState	From the pull-down menu, select whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

OperCtlState	This displays whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.
Port Control	From the pull-down menu, select Force Authorized, Force Unauthorized or Auto – Force Authorized forces the Authenticator of the port to become Authorized. Force Unauthorized forces the port to become Unauthorized.
Quiet Period	Select the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Select the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.
Support Timeout	Select the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.
Server Timeout	Select the length of time to wait for a response from a Radius server.
MaxReq	Select the maximum number of times to retry sending packets to the supplicant.
ReAuthPeriod	Select the time interval between successive re-authentications.

ReAuthenticate	Enable or disable reauthentication.

Radius Server Settings

Use this menu to configure the settings the switch will use to communicate with a Radius server. To add Radius server settings click the New button, a separate configuration menu appears. To edit an existing Radius settings index, select it and click the edit button

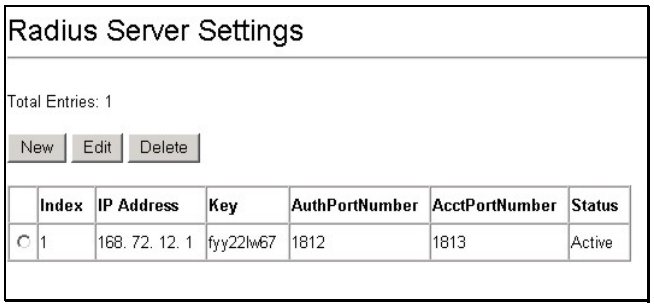


Figure 6 - 65. Radius Server Settings

The parameters configured for adding and editing Radius settings are the same. See the table below for a description.

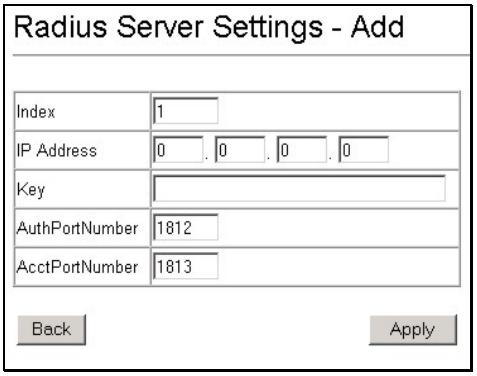


Figure 6 - 66. Radius Server – Add New

Configure the following Radius server settings:

Parameter	Description
Index	Radius server settings index.
IP Address	Type in the IP address of the Radius server.
Key	Type the shared-secret key used by the Radius server and the switch. Up to 32 characters can be used.
AuthPortNumber	Type the UDP port number for authentication requests. The default is 1812.
AcctPortNumber	Type the UDP port number for accounting requests (if accounting server is being used). The default is 1813.

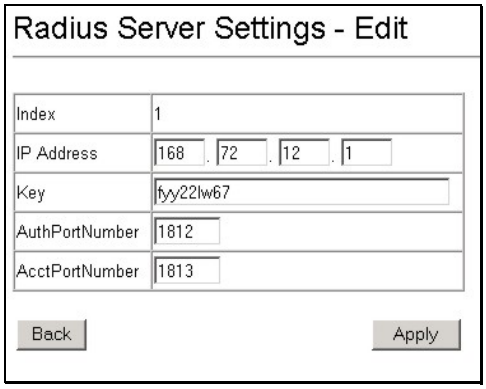


Figure 6 - 67. Edit Radius Server Settings

802.1X State

To enable 802.1x on the switch select *Enabled* and click the Apply button.

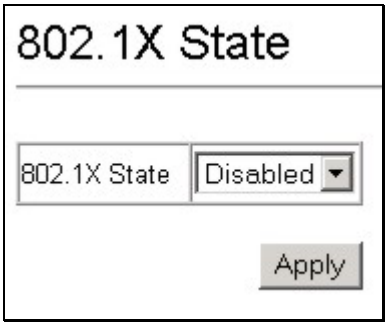


Figure 6 - 68. 802.1X State – Enable/Disable

Access Profile Mask

Access profiles allow you to establish criteria to determine whether or not the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address or IP address.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the switch will use to determine what to do with the frame. The entire process is described below in two parts.

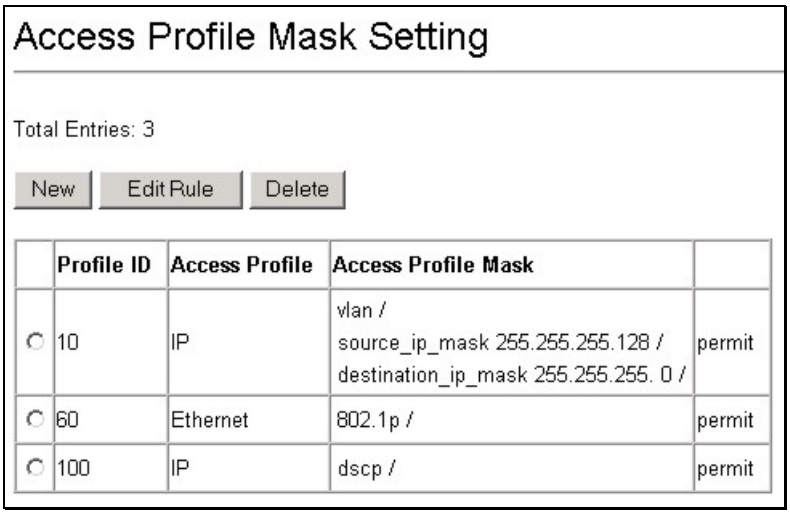


Figure 6 - 69. Access Profile Mask Setting Table

To create an Access Profile Mask:

Click the New button in the Access Profile Mask Setting summary table page. A new menu is displayed. Use this to create an access profile and specify what criteria are used to examine frames. Once the profile has been created you can set up the rule applied to the profile as described later in this section.

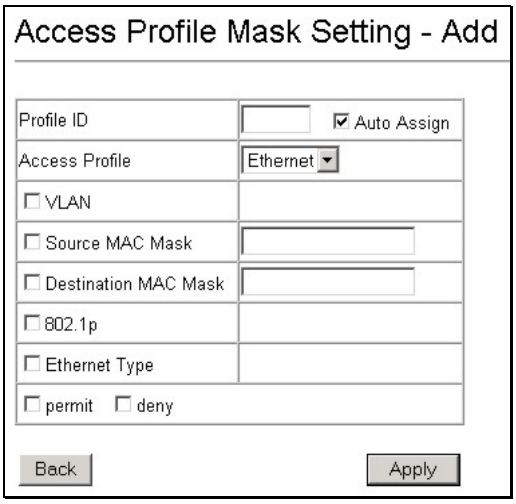


Figure 6 - 70. MAC Address Access Profile Mask Setting – Add

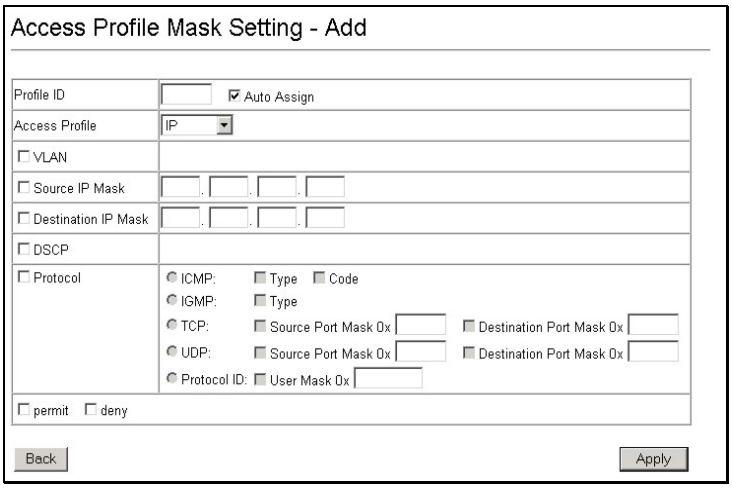


Figure 6 - 71. IP Address Access Profile Mask – Add

Configure the following Access Profile Mask settings:

Parameter	Description
Profile ID	Type in a unique identifier number for this profile set or allow an ID to be automatically assigned by checking the Auto Assign option. This value can be set from 1 – 255.
Access Profile	Select profile based on Ethernet (MAC Address) or IP address. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the switch to examine the layer 2 part of each packet header. Select IP to instruct the switch to examine the IP address in each frame's header.
VLAN	Selecting this option instructs the switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
Source MAC/IP Mask	Source MAC Mask - Enter a MAC address mask for the source MAC address. Source IP Mask - Enter an IP address mask for the source IP address.
Destination MAC/IP Mask	Destination MAC Mask - Enter a MAC address mask for the destination MAC address. Destination IP Mask - Enter an IP address mask for the destination MAC address.
802.1p	Selecting this option instructs the switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.

DSCP	Selecting this option instructs the switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type (for Ethernet Access Profiles only)	Selecting this option instructs the switch to examine the Ethernet type value in each frame's header.
Protocol (for IP address Access Profiles only)	Selecting this option instructs the switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines: Select **ICMP** to instruct the switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select **Type** to further specify that the access profile will apply an ICMP type value, or specify **Code** to further specify that the access profile will apply an ICMP cod value. Select **IGMP** to instruct the switch to examine the Internet Group Management Protocol (ICMP) field in each frame's header. Select **Type** to further specify that the access profile will apply an IGMP type value Select **TCP** to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP

	requires that you specify a source port mask and/or a destination port mask. **Source Port Mask Ox** - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff). **Destination Port Mask Ox** - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff). Select **UDP** to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. **Source Port Mask Ox** - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff). **Destination Port Mask Ox** - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff).
Permit/Deny	Select permit to specify that the packets that match the access profile are forwarded by the switch according to any additional rule added (see below). Select deny to specify that packets that do not match the access profile are not forwarded by the switch and will be filtered.

To establish the rule for a previously created Access Profile Mask:

Select the Access Profile from the Access Profile Mask Setting Table and click the Edit Rule button.

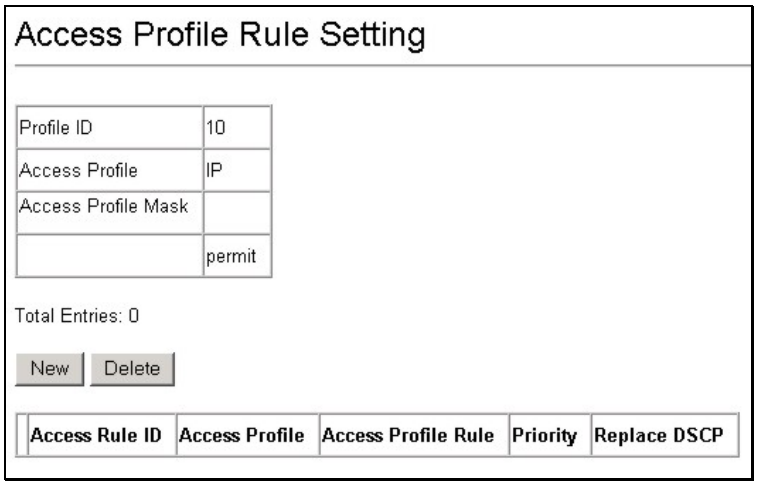


Figure 6 - 72. Access Profile Rule Setting

To create a new rule set for the access profile click the New button. A new menu is displayed. To remove a previously created rule, select it and lick the Delete button.

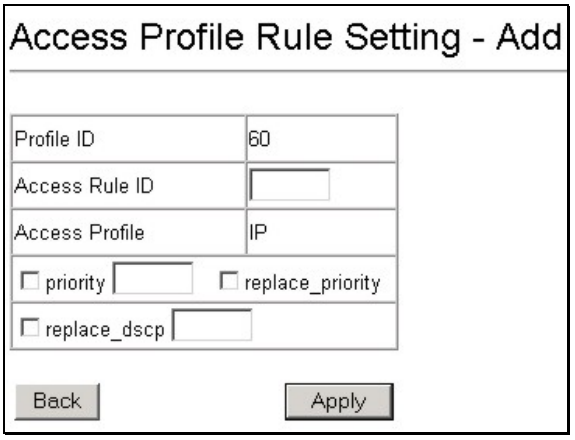


Figure 6 - 73. Add Access Profile Rule

Configure the following Access Profile Rule settings:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Access Rule ID	Type in a unique identifier number for this access. This value can be set from 1 – 255.
priority	Select this option to instruct the switch to use the 802.1p priority value entered in the adjacent field for packets that meet the criteria. A number between 0 – lowest priority, and 7 – highest priority, can be entered.
replace_priority	Select this option to instruct the switch to replace the 802.1p value (in a packet that meets the selected criteria). In this way, packets meeting the criteria can have their priority handling modified for use within the switch, and then have a different priority value assigned when they leave the switch.
replace_dscp:	Select this option to instruct the switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.

System Log Server

The switch can send Syslog messages to up to four designated servers. Use the System Log Server

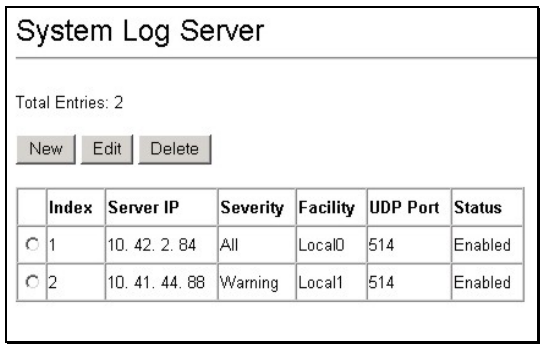


Figure 6 - 74. System Log Server list

The parameters configured for adding and editing System Log Server settings are the same. See the table below for a description.

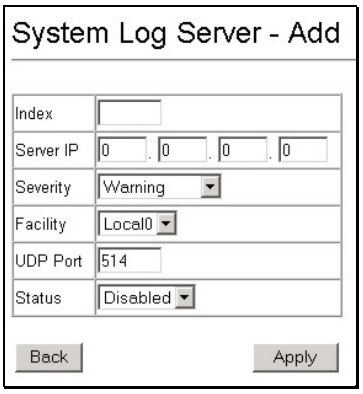


Figure 6 - 75. System Log Server – Add menu

Parameter	Description
Index	Syslog server settings index (1-4).
Server IP	Type in the IP address of the Syslog server receiving the message.
Severity	Select the level of message sent, select: *Warning*, *Information* or *All*.
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now. Numerical Code — Facility 0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog line printer subsystem 7 network news subsystem 8 UUCP subsystem 9 clock daemon 10 security/authorization

	messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon **16 local use 0 (local0)** **17 local use 1 (local1)** **18 local use 2 (local2)** **19 local use 3 (local3)** **20 local use 4 (local4)** **21 local use 5 (local5)** **22 local use 6 (local6)** **23 local use 7 (local7)**
UDP Port	Type the UDP port number used for sending Syslog messages. The default is 514.
Status	Choose Enabled or Disabled to activate or deactivate this

System Log State

To enable the System Log Server settings you have chosen select *Enabled* and click the Apply button in the System Log State menu.

Figure 6 - 76. System Log State menu

IGMP Snooping Settings

To configure IGMP Snooping:

Click **IGMP Snooping Configurations** to open the following dialog box:

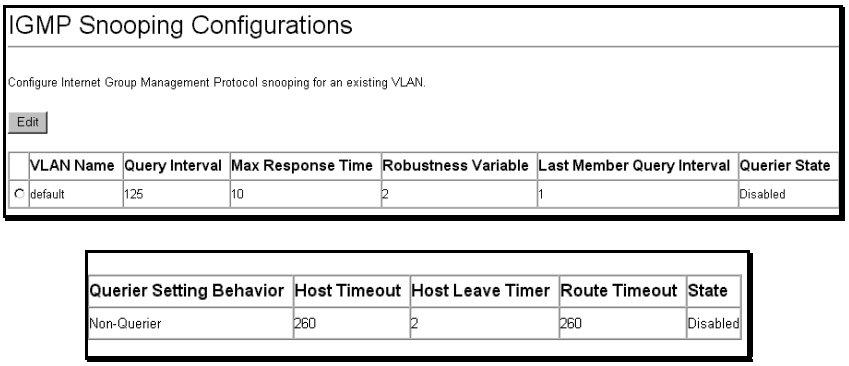


Figure 6 - 77. IGMP Snooping Configuration

To edit an IGMP Snooping entry on the switch, select the entry on the IGMP Snooping Configurations screen and then click the edit button:

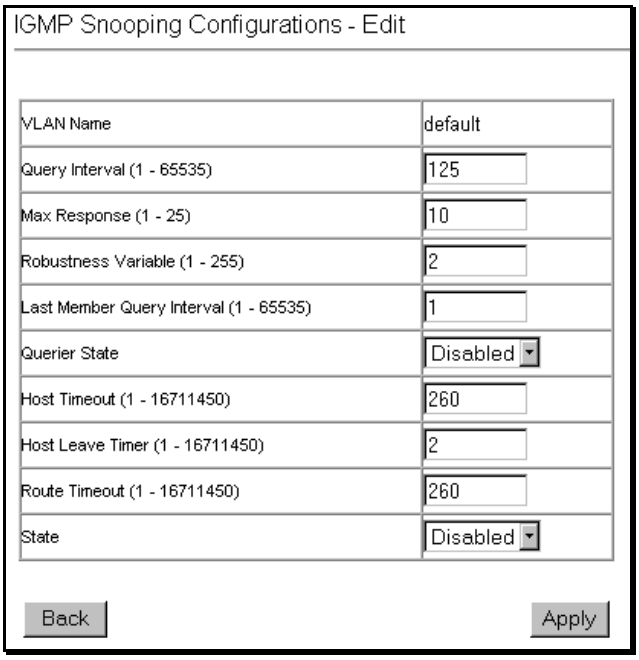


Figure 6 - 78. IGMP Snooping Configuration

The following fields can be set:

Parameter	Description
VLAN Name	Allows the entry of the name of the VLAN for which IGMP Snooping is to be configured.
Query Interval	Allows the entry of a value between 1 and 65500 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.

Max Response	Sets the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered, with a default of 10 seconds.
Robustness Variable	A tuning variable to allow for sub-networks that are expected to lose a large number of packets. A value between 2 and 255 can be entered, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.
Last Member Query Interval	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is 1 second.
Querier State	This field can be switched using the pull-down menu between *Disabled* and *Enabled*.
Host Timeout	Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.

Host Leave Timer	Specifies the maximum amount of time between the switch receiving a leave group message from a host, and the switch issuing a group membership query. If the switch does not receive a response from the group membership query before the Host Leave Timer expires, the host address is deleted from the switch's forwarding table. The default is 2 seconds.
Route Timeout	Specifies the maximum amount of time a route will remain in the switch's forwarding table without receiving a membership report. The default is 260 seconds.
State <*Disabled*>	This field can be switched using the pull-down menu between *Disabled* and *Enabled*. This is used to enable or disable IGMP Snooping for the specified VLAN.

Utilities

TFTP Utilities

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

Note: To get the latest firmware for the switch go to the D-Link website: www.dlink.com

Update Firmware from Server

To update the switch's firmware, click on the Basic Setup folder and then the Switch Utilities folder and then the TFTP Services folder and finally click on the Download Firmware from TFTP Server link:

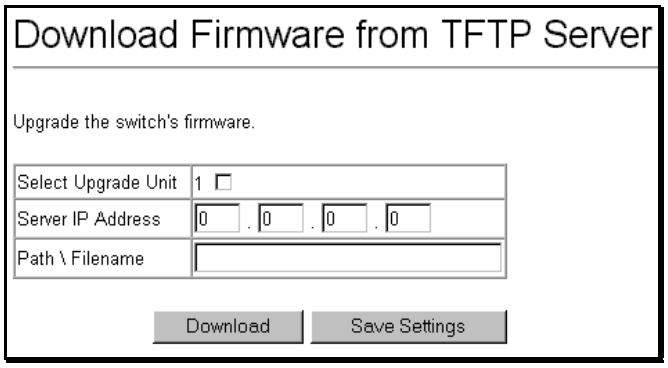


Figure 6 - 79. Download Firmware from Server

Select which switch of a switch stack you want to update the firmware on. This allows the selection of a particular switch from a switch stack if you have installed the optional stacking module and have properly interconnected the switches.

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

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

Enter the path and the filename to the firmware file on the TFTP server. Note that in the above example, the firmware file is in the root directory of the D drive of the TFTP server.

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

Click **Download** to record the IP address of the TFTP server. Use the **Save Settings** to enter the address into NV-RAM.

Click **Start** to initiate the file transfer.

Use Configuration File on Server

To download a configuration file for the switch's, click on the Basic Setup folder and then the Switch Utilities folder and then the TFTP Services folder and finally click on the Download Configuration from TFTP Server link:

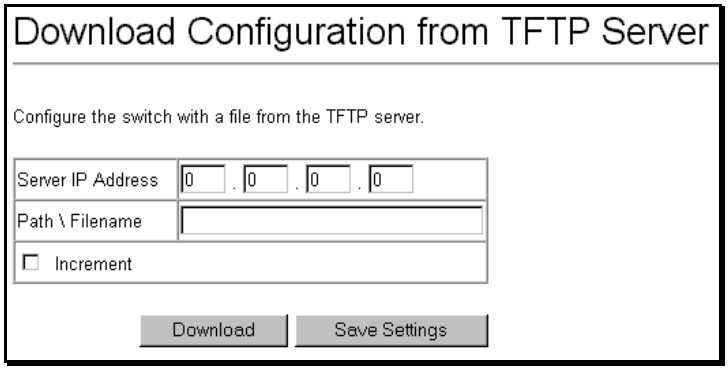


Figure 6 - 80. Use Configuration File on Server

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

Click **Apply** to record the IP address of the TFTP server. Use **Save Changes** from the **Maintenance** menu to enter the address into NV-RAM

Click **Start** to initiate the file transfer.

Save Settings To Server

To download a configuration file for the switch's, click on the Basic Setup folder and then the Switch Utilities folder and then the TFTP Services folder and finally click on the Upload Settings to TFTP Server link:

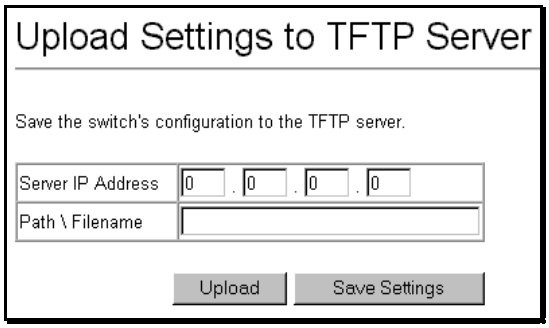


Figure 6 - 81. Save Settings To TFTP Server

Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server and click **Apply**. Highlight **Start** to initiate the file transfer.

Save History Log to Server

To download a configuration file for the switch's, click on the Basic Setup folder and then the Switch Utilities folder and then the TFTP Services folder and finally click on the Upload history Log to TFTP Server link:

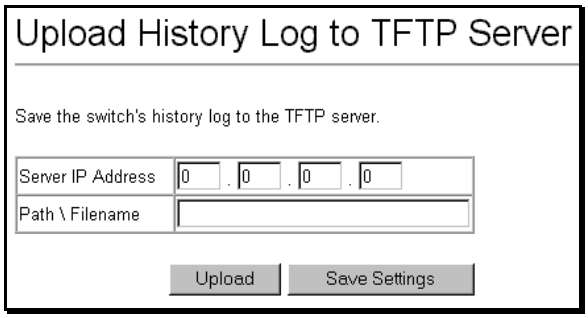


Figure 6 - 82. Save Switch History To TFTP Server

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. Click **Apply** to make the changes current. Click **Start** to initiate the file transfer.

Utilities

Ping Test

Ping is a small program that sends data packets to the IP address you specify. The destination node then returns the packets to the switch. This is very useful to verify connectivity between the switch and other nodes on the network.

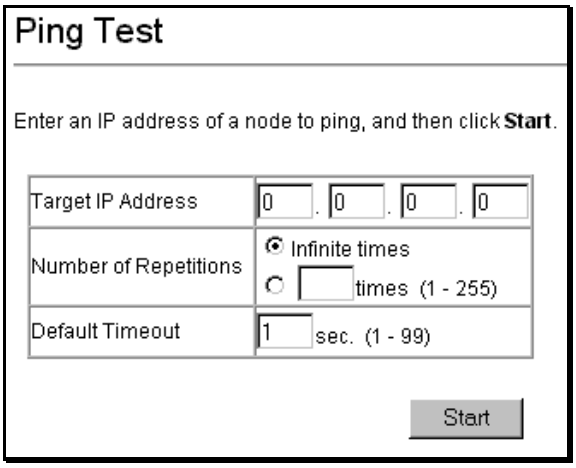


Figure 6 - 83. Ping Test Screen

The **Infinite times** checkbox, in the **Number of Repetitions** field, tells ping to keep sending data packets to the specified IP address until the program is stopped.

Network Monitoring

The DES-3226S provides extensive network monitoring capabilities that can be viewed from the under **Network Monitoring** menu.

Port Utilization

The **Port Utilization** window shows the percentage of the total available bandwidth being used on the port. Port utilization statistics may be viewed using a line graph or table format.

To view the port utilization, click on the Network Monitoring folder and then the Statistics folder and then the Port Utilization link:

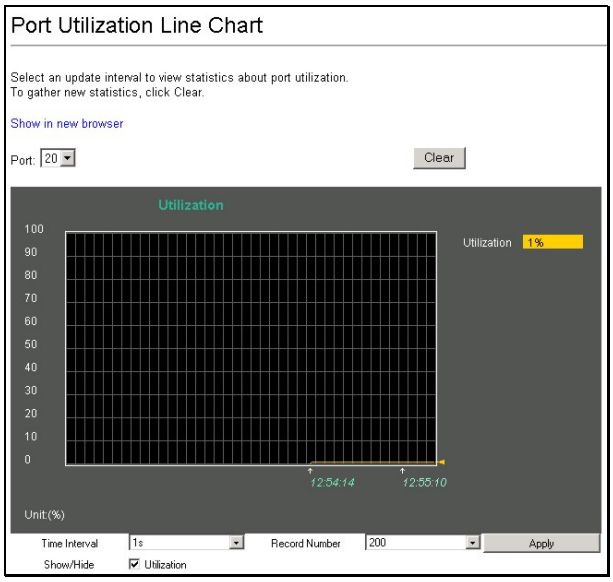


Figure 6 - 84. Port Utilization Line Chart

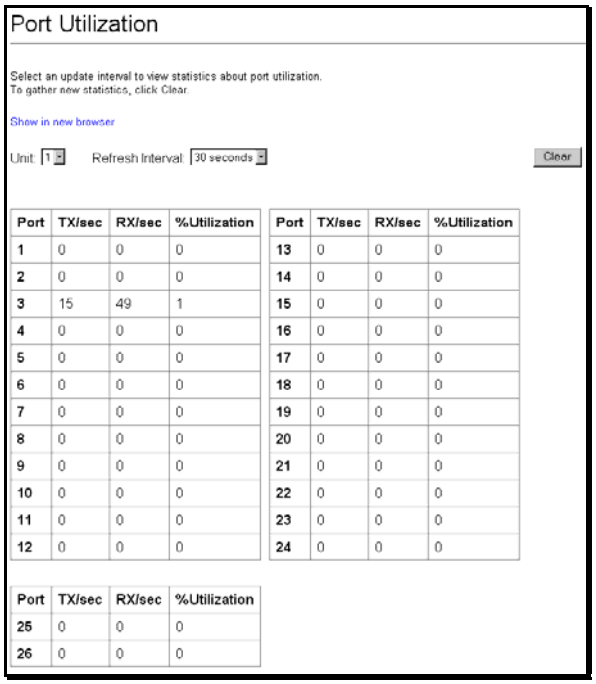


Figure 6 - 85. Port Utilization Table

Select the desired port by clicking on the front panel display. The **Update Interval** field sets the interval at which the error statistics are updated.

The following field can be set:

Parameter	Description
Update Interval <*Suspend*>	The time between updates received from the switch, in seconds. *Suspend* stops the updates. The default is *Suspend*.

Port Error Statistics

The **Port Error Packet Statistics** window displays the packet errors that the switch can detect and displays the results on a per port basis.

To view the error statistics for a port, click on the Port Error Packets link:

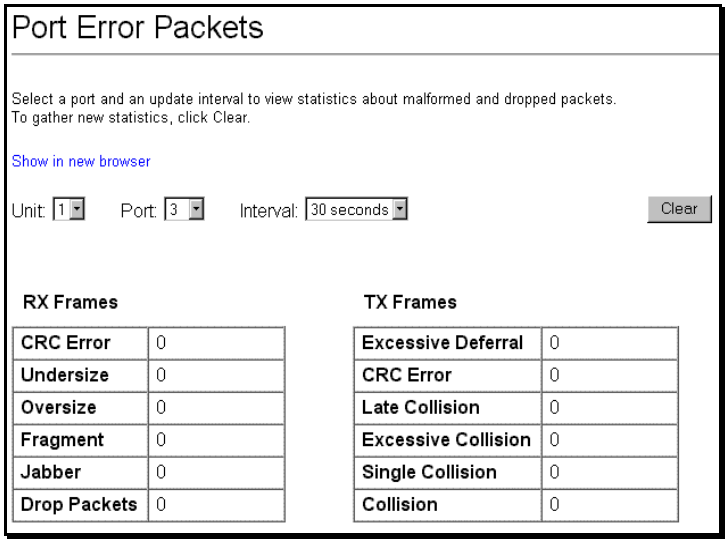


Figure 6 - 86. Port Error Packet Statistics window

Select the desired port by clicking on the front panel display. The **Update Interval** field sets the interval at which the error statistics are updated.

The following fields from above are described in more detail:

Parameter	Description
Unit	Allows the selection of a particular switch in a switch stack if you have installed the optional stacking module and have properly interconnected the switches.
Port	Allows the selection of a particular port on the switch.
Update Interval <*Suspend*>	The interval (in seconds) that the table is updated. The default is *Suspend.*
RX Frames	Received packets.
CRC Error	For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
Undersize	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Fragment	The total number of frames received that were less that 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or an alignment error.
Jabber	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or an alignment error.
Drop Packets	The total number of events in which packets were dropped due to a lack of resources.
TX Frames	Transmitted packets.
Excessive Deferral	The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
Late Collision	Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collision	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.

Single Collision	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.

Port Packet Analysis

The **Port Packet Analysis** window displays the size of packets received or transmitted by a given switch port. In addition, statistics on the number and rate of unicast, multicast, and broadcast packets received by the switch are displayed.

To view an analysis of packets received or transmitted by a port, click on the Port Packet Analysis link:

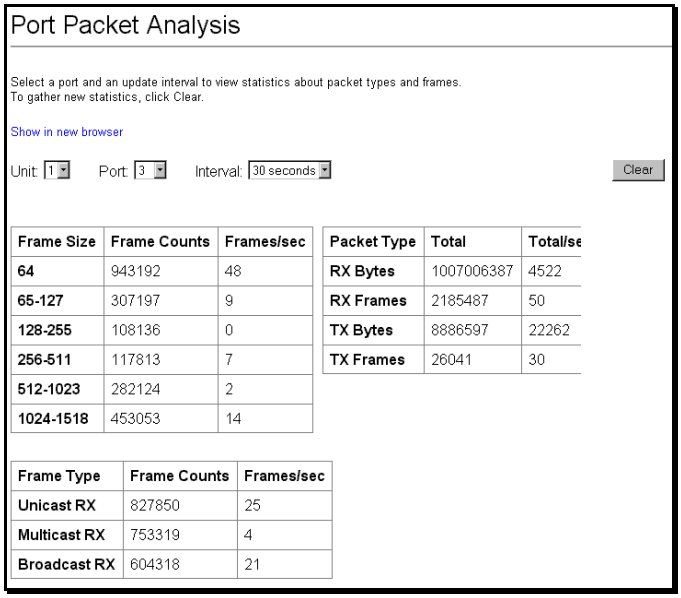


Figure 6 - 87. Port Packet Analysis window

The following fields from above are described in more detail:

Parameter	Description
Update Interval <*Suspend*>	The interval (in seconds) that the table is updated. The default is 2 seconds.
Frames	The number of packets (or frames) received or transmitted by the switch with the size, in octets, given by the column on the right.
Frames/sec	The number of packets (or frames) transmitted or received, per second, by the switch.
Unicast RX	Displays the number of unicast packets received by the switch in total number (**Frames**) and the rate (**Frames/sec**).
Multicast RX	Displays the number of multicast packets received by the switch in total number (**Frames**) and the rate (**Frames/sec**).
Broadcast RX	Displays the number of broadcast packets received by the switch in total number (**Frames**) and the rate (**Frames/sec**).
RX Bytes	Displays the number of bytes (octets) received by the switch in total number (**Total**), and rate (**Total/sec**).
RX Frames	Displays the number of packets (frames) received by the switch in total

	number (**Total**), and rate (**Total/sec**).
TX Bytes	Displays the number of bytes (octets) transmitted by the switch in total number (**Total**), and rate (**Total/sec**).
TX Frames	Displays the number of packets (frames) transmitted by the switch in total number (**Total**), and rate (**Total/sec**).

MAC Address Table

This allows the switch's dynamic MAC address forwarding table to be viewed. When the switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the switch.

To view the MAC address forwarding table, from the Address Tables folder, click the MAC Address Table link:

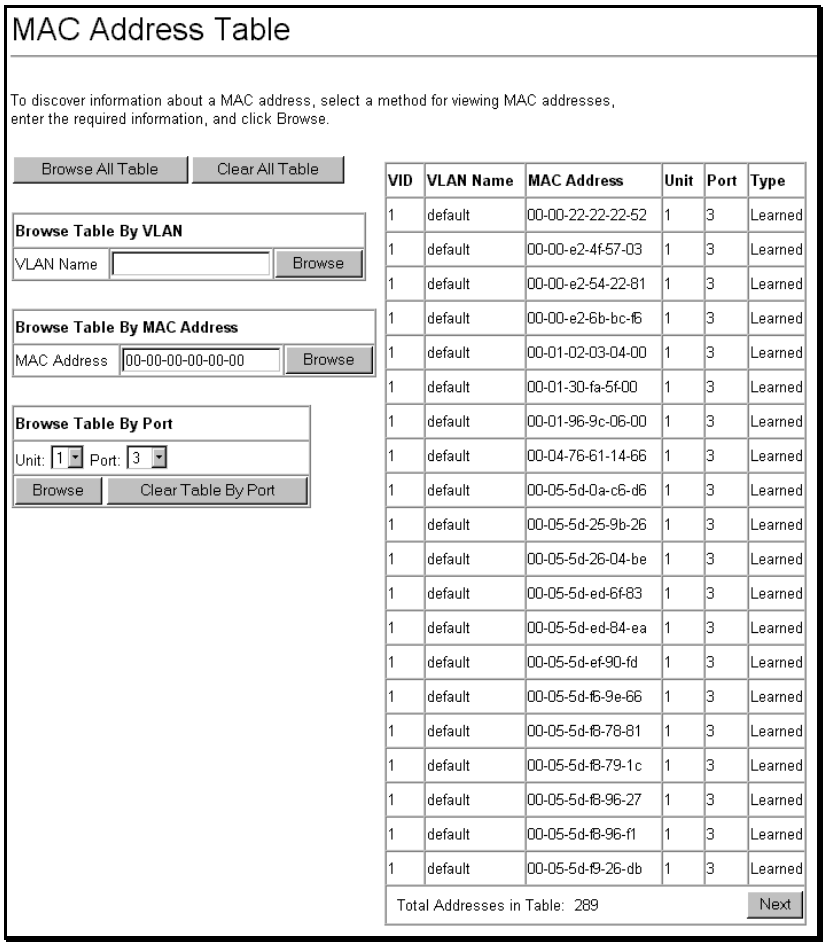


Figure 6 - 88. Browse Address Table – sequential window

GVRP Status

This allows the GVRP status for each of the switch's ports to be viewed by VLAN. The GVRP status screen displays the ports on the switch that are currently Egress or Untagged ports.

To view the GVRP status table, click on the GVRP Status link:

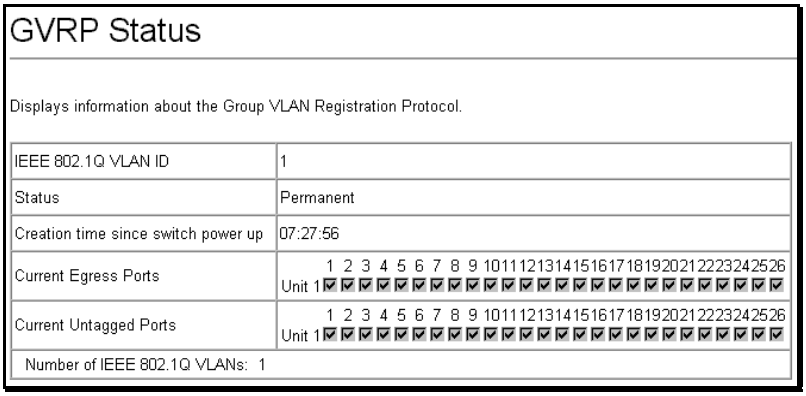


Figure 6 - 89. GVRP Status

Router Ports

This displays which of the switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by **S**. A router port that is dynamically configured by the switch is designated by **D**.

To view the Router Port table, click on the Router Ports link:

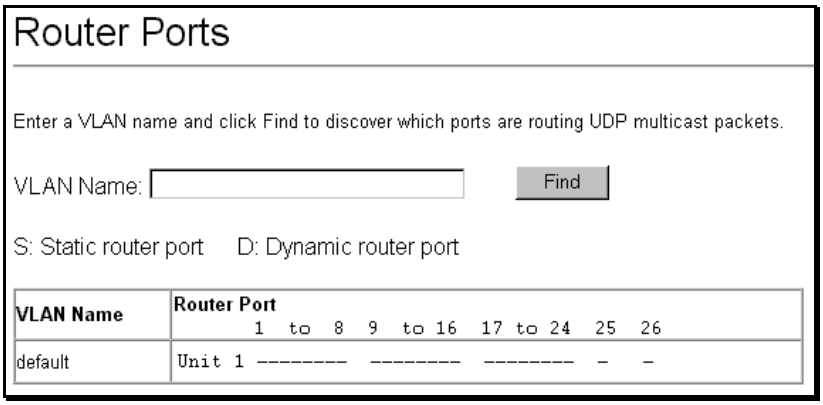


Figure 6 - 90. Browse Router Port

S signifies a static router port, configured by the user.

D signifies a dynamically assigned router port, configured by the switch.

IGMP Snooping Status

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

To view the IGMP Snooping table, click on the IGMP Snooping Status link:

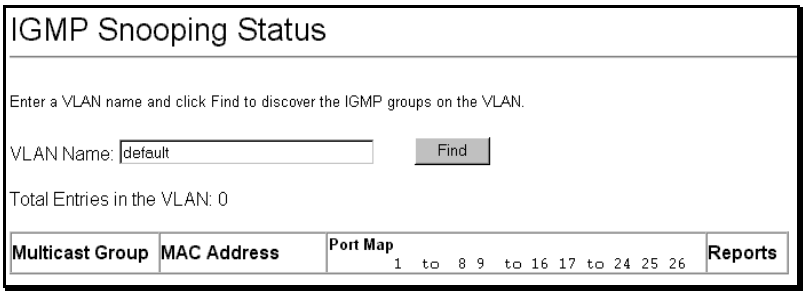


Figure 6 - 91. IGMP Snooping Status

The following fields can be set or are displayed.

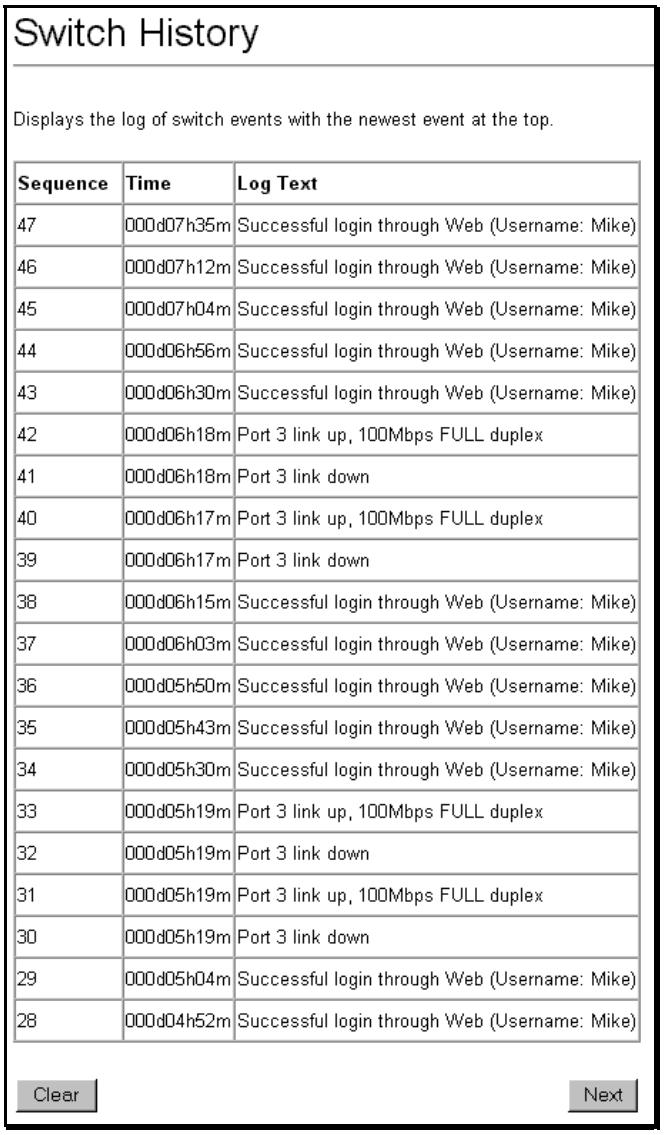
Parameter	Description
Multicast Group	The IP address of the multicast group.
MAC Address	The MAC address of the multicast group.
Reports	The total number of reports received for this group.

Switch History

This allows the Switch History Log to be viewed. The switch records all traps, in sequence, that identify events on the switch. The time since the last cold start of the switch is also recorded.

To view the switch history log:

Click the **Switch History** link on the **Applications** menu:



Switch History

Displays the log of switch events with the newest event at the top.

Sequence	Time	Log Text
47	000d07h35m	Successful login through Web (Username: Mike)
46	000d07h12m	Successful login through Web (Username: Mike)
45	000d07h04m	Successful login through Web (Username: Mike)
44	000d06h56m	Successful login through Web (Username: Mike)
43	000d06h30m	Successful login through Web (Username: Mike)
42	000d06h18m	Port 3 link up, 100Mbps FULL duplex
41	000d06h18m	Port 3 link down
40	000d06h17m	Port 3 link up, 100Mbps FULL duplex
39	000d06h17m	Port 3 link down
38	000d06h15m	Successful login through Web (Username: Mike)
37	000d06h03m	Successful login through Web (Username: Mike)
36	000d05h50m	Successful login through Web (Username: Mike)
35	000d05h43m	Successful login through Web (Username: Mike)
34	000d05h30m	Successful login through Web (Username: Mike)
33	000d05h19m	Port 3 link up, 100Mbps FULL duplex
32	000d05h19m	Port 3 link down
31	000d05h19m	Port 3 link up, 100Mbps FULL duplex
30	000d05h19m	Port 3 link down
29	000d05h04m	Successful login through Web (Username: Mike)
28	000d04h52m	Successful login through Web (Username: Mike)

Clear Next

Figure 6 - 92. Switch History

A

TECHNICAL SPECIFICATIONS

	General	
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX Gigabit Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	n/a	2000Mbps
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 UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
Fiber Optic:	IEC 793-2:1992 Type A1a - 50/125um multimode Type A1b - 62.5/125um multimode Both types use SC optical connector
Number of Ports:	24 x 10/100 Mbps NWay ports 2 Gigabit Ethernet (optional)

Physical and Environmental	
AC inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	29 watts maximum
DC fans:	2 built-in 40 x 40 x10 mm fans
Operating Temperature:	0 to 50 degrees Celsius
Storage Temperature:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width

Physical and Environmental	
Weight:	2.5 kg
EMI:	FCC Class A, CE Class A, VCCI Class A, BSMI Class A, C-Tick Class A FCC Part 15/IECES-003 (Canada), VCCI Class A ITE, EN55022/EN50082-1 or EN55024, C-Tick (AS/NZS3548, BSMI (CNS 13438)
Safety:	UL, CSA, CE Mark, TUV/GS, CSA International

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	8 MB per device
Filtering Address Table:	8K MAC address per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,000 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 300 - 1000000 seconds. Default = 300.

B

BITWISE LOGICAL OPERATIONS

AND

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

	0	***1***
0	0	0
1	0	1

OR

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

	0	***1***
0	0	1
1	1	1

XOR

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

	0	***1***
0	0	1
1	1	0

NOT

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

0	***1***
1	0

INDEX

D-Link® Offices

Australia

D-Link Australasia
1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia
TEL: 61-2-8899-1800 FAX: 61-2-8899-1868
TOLL FREE (Australia): 1300 766 868
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au & info@dlink.com.au

Brazil

D-Link Brasil Ltda.
Rua Tavares Cabral 102 - Conj. 31 e 33
05423-030 Pinheiros, Sao Paulo, Brasil
TEL: (5511) 3094 2910 to 2920 FAX: (5511) 3094 2921
URL: www.dlink.com.br

Canada

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

Chile

D-Link South America (Sudamérica)
Isidora Goyenechea 2934
Oficina 702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-232-0923
URL: www.dlink.com.cl

China

D-Link Beijing
Level 5,Tower W1,The Tower,Oriental Plaza
No.1,East Chang An Ave., Dong Cheng District
Beijing,100738,China
TEL: (8610) 85182529/30/31/32/33
FAX: (8610) 85182250
URL: www.dlink.com.cn E-MAIL: webmaster@dlink.com.cn

Denmark

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

Egypt

D-Link Middle East
7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt
TEL: 202-624-4615 FAX: 202-624-583
URL: www.dlink-me.com
E-MAIL: support@dlink-me.com
& dlinkegypt@dlink-me.com

Finland **D-Link Finland**
Pakkalankuja 7A, 01510 Vantaa, Finland
TEL: 358-9-2707-5080 FAX: 358-9-2707-5081
URL: www.dlink-fi.com

France **D-Link France**
Le Florilege, No. 2, Allée de la Fresnerie,
78330 Fontenay-le-Fleury, France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689
URL: www.dlink-france.fr
E-MAIL: info@dlink-france.fr

Germany **D-Link Central Europe (D-Link Deutschland GmbH)**
Schwalbacher Strasse 74, D-65760 Eschborn, Germany
TEL: 49-6196-77990 FAX: 49-6196-7799300
BBS: 49-(0) 6192-971199 (analog)
& BBS: 49-(0) 6192-971198 (ISDN)
INFO: 00800-7250-0000 (toll free)
& HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 & HELP: support.dlink.de
URL: www.dlink.de & E-MAIL: info@dlink.de

India **D-Link India**
Plot No.5, Kurla -Bandra Complex Rd., Off Cst Rd.,
Santacruz (East), Mumbai, 400 098 India
TEL: 91-022-2652-6696/6788/6623
FAX: 91-022-2652-8914/8476
URL: www.dlink.co.in
E-MAIL: service@dlink.co.in & tushars@dlink.co.in

Italy **D-Link Mediterraneo Srl/D-Link Italia**
Via Nino Bonnet n. 6/B, 20154, Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723
URL: www.dlink.it E-MAIL: info@dlink.it

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

Netherlands **D-Link Benelux**
Lichtenauerlaan 102-120, 3062 ME Rotterdam, Netherlands
TEL: +31-10-2045740 FAX: +31-10-2045880
URL: www.d-link-benelux.nl & www.dlink-benelux.be
E-MAIL: info@dlink-benelux.com

Norway	**D-Link Norway** Karihaugveien 89, 1086 Oslo TEL: 47-22-309075 FAX: 47-22-309085 SUPPORT: 800-10-610 & 800-10-240 (DI-xxx) URL: www.dlink.no
Russia	**D-Link Russia** 129626 Russia, Moscow, Graphskiy per., 14, floor 6 TEL/FAX: +7 (095) 744-00-99 URL: www.dlink.ru E-MAIL: vl@dlink.ru
Singapore	**D-Link International** 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-6774-6233 FAX: 65-6774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com
South Africa	**D-Link South Africa** Einstein Park II, Block B 102-106 Witch-Hazel Avenue Highveld Technopark Centurion, Gauteng, Republic of South Africa TEL: +27-12-665-2165 FAX: +27-12-665-2186 URL: www.d-link.co.za E-MAIL: attie@d-link.co.za
Spain	**D-Link Iberia S.L.** Sabino de Arana, 56 bajos, 08028 Barcelona, Spain TEL: 34 93 409 0770 FAX: 34 93 491 0795 URL: www.dlink.es E-MAIL: info@dlink.es
Sweden	**D-Link Sweden** P. O. Box 15036, S-167 15 Bromma, Sweden TEL: 46-8-564-61900 FAX: 46-8-564-61901 URL: www.dlink.se 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 URL: www.dlinktw.com.tw E-MAIL: dssqa@dlinktw.com.tw
Turkey	**D-Link Turkiye** Beybi Giz Plaza, Ayazaga Mah. Meydan Sok. No. 28 Maslak 34396, Istanbul-Turkiye TEL: 90-212-335-2553 (direct) & 90-212-335-2525 (pbx) FAX: 90-212-335-2500 E-MAIL: dlinkturkey@dlink-me.com E-MAIL: support@dlink-me.com

U.A.E. **D-Link Middle East FZCO**
P.O. Box18224 R/8, Warehouse UB-5
Jebel Ali Free Zone, Dubai – United Arab Emirates
TEL: (Jebel Ali): 971-4-883-4234
FAX: (Jebel Ali): 971-4-883-4394
& (Dubai): 971-4-335-2464
E-MAIL: dlinkme@dlink-me.com & support@dlink-me.com

U.K. **D-Link Europe (United Kingdom) Ltd**
4th Floor, Merit House, Edgware Road, Colindale, London
NW9 5AB United Kingdom
TEL: 44-020-8731-5555 SALES: 44-020-8731-5550
FAX: 44-020-8731-5511 SALES: 44-020-8731-5551
BBS: 44 (0) 181-235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

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

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____

Organization: _____ Dept. _____

Your title at organization: _____

Telephone: _____ Fax:_____

Organization's full address: _____

_____

Country: _____

Date of purchase (Month/Day/Year): _____

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

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____

Telephone: _____ Fax:_____

Reseller's full address: _____

_____

_____

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

1. Where and how will the product primarily be used?

☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?

☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?

☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?

☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others_____

5. What network management program does your organization use ?

☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others_____

6. What network medium/media does your organization use ?

☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other_____

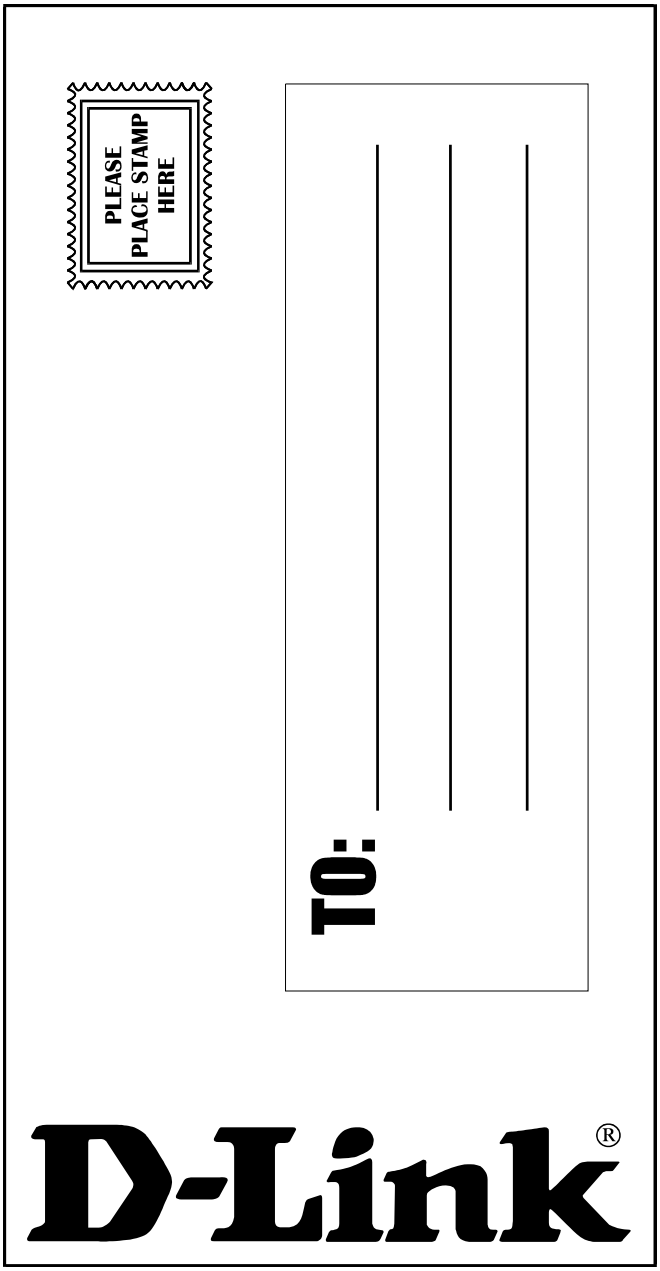
9. Would you recommend your D-Link product to a friend?

☐Yes ☐No ☐Don't know yet

10.Your comments on this product?

_____

_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®