

DES-3210/DES-3218/DES-3226

Managed Standalone Fast Ethernet Switch
User's Guide

Third Edition (June 2003)

651ES3226035

Printed In Taiwan



RECYCLABLE

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehöerteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät 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 sollte auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a –Netz Kabel oder Netzstecker sind beschädigt.
 - b –Flüssigkeit ist in das Gerät eingedrungen.
 - c –Das Gerät war Feuchtigkeit ausgesetzt.
 - d –Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e –Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Originalersatzteile bzw. den Originalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Reparatur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm² einzusetzen.

Trademarks

Copyright D-Link Corporation ©2003. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

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

Limited Warranty

Hardware:

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

Product Type	Warranty Period
Complete products	One year
Spare parts and spare kits	90 days

The one-year period of warranty on complete products applies on condition that the product's Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. Failing such timely registration of purchase, the warranty period shall be limited to 90 days.

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

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

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

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

Software:

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

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

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

LIMITATION OF WARRANTIES

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

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

LIMITATION OF LIABILITY

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

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

D-Link Offices for Registration and Warranty Service

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

FCC Warning

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

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

CE Mark Warning

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

Warnung!

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

Precaución!

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

Attention!

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

Attenzione!

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

VCCI Warning

注意

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

BSMI Warning

警告使用者

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

Table of Contents

About This Guide.....	1
Overview of this User's Guide.....	1
Introduction.....	2
Features.....	2
Ports.....	2
Performance Features.....	2
Management.....	3
Unpacking and Setup.....	5
Unpacking.....	5
Installation.....	5
Desktop or Shelf Installation.....	5
Rack Installation.....	6
Power on.....	7
Power Failure.....	7
Identifying External Components.....	8
Front Panel.....	8
Rear Panel.....	8
Side Panels.....	9
Optional 100BASE and 1000BASE Extension Modules.....	9
LED Indicators.....	12
Connecting The Switch.....	13
Switch to End Node.....	13
Switch to Hub or Switch.....	13
Switch Management and Operating Concepts.....	14
Local Console Management.....	14
Diagnostic (console) port (RS-232 DCE).....	14
IP Addresses and SNMP Community Names.....	15
Traps.....	16
MIBs.....	16
SNMP.....	17
Authentication.....	17
Packet Forwarding.....	17
MAC Address Aging Time.....	17
Filtering.....	18
Spanning Tree Protocol.....	18
STP Operation Levels.....	18
Bridge Protocol Data Units.....	19
Creating a Stable STP Topology.....	20

STP Port States.....	20
User-Changeable STP Parameters.....	21
Illustration of STP	22
VLANs	23
Notes About VLANs on the DES-3210/DES-3218/DES-3226	23
IEEE 802.1Q VLANs.....	24
802.1Q VLAN Packet Forwarding.....	24
802.1Q VLAN Tags	25
Port VLAN ID.....	26
Tagging and Untagging.....	27
Ingress Filtering	27
VLANs	27
DHCP	28
802.1X Port-based Network Access Control	29
Configuring the Switch Using the Console Interface.....	32
Before You Start	32
Connecting to the Switch	32
User Accounts Management	34
Save Changes	36
Factory Reset.....	37
Configuration	40
Configure IP Address.....	40
Configure Switch Information and Advanced Settings.....	42
Configure Ports	43
Configure Bandwidth	44
Configure Spanning Tree Protocol.....	46
Configure Static (Destination-Address Filtering) Table	48
Configure VLANs.....	49
Configure IGMP Snooping	53
Configure Port LACP Trunking.....	54
Configure Port Mirroring	56
Configure Threshold of Broadcast/Multicast/DA-Unknown Storm	56
Configure Class of Service, Default Priority and Traffic Class	57
Configure Port GMRP Settings.....	59
Configure DIFFSERV Settings.....	60
Security Management.....	60
Configure Port Security.....	61
Configure Port Access Entity	61
Security IP	67
Secure Shell.....	68
Access Authentication Control.....	69

Network Monitoring.....	71
Port Utilization.....	71
Port Error Packets.....	72
Port Packet Analysis.....	72
Browse MAC Address.....	73
Switch History.....	73
IGMP Snooping.....	74
Dynamic Group Registration Table.....	74
VLAN Status.....	75
Port Access Control Statistics.....	75
SNMP Manager Configuration.....	79
SNMP V1 & V2.....	79
SNMP V3.....	81
System Utilities.....	91
Upgrade Firmware from TFTP Server.....	92
Use Configuration File on TFTP Server.....	93
Save Settings to TFTP Server.....	93
Save History Log to TFTP Server.....	94
Download Hostkey Certificate File.....	94
Ping Test.....	95
Reboot.....	95
Web-Based Network Management.....	97
Introduction.....	97
Getting Started.....	97
Configuration.....	99
IP Address.....	99
Switch Information.....	100
Advanced Settings.....	101
Port Configuration.....	103
Port Mirroring.....	104
Port LACP Trunking.....	105
IGMP Snooping.....	106
Port GMRP.....	107
Diffserv Settings.....	108
Spanning Tree.....	109
Static Filtering Table.....	111
VLANs.....	112
Port Bandwidth.....	114
Threshold of Broadcast.....	115
Port Priority.....	116
Class of Traffic.....	117

Class of Service.....	117
Security Management.....	117
Port Security.....	118
Security IP.....	118
PAE Access Entity.....	120
Radius Server.....	125
Secure Shell.....	127
Access Authentication Control.....	129
User Account Management.....	130
SNMP Manager.....	130
SNMP V1&V2.....	131
SNMP V1&V2&V3.....	132
Monitoring.....	141
Port Utilization.....	141
Packets.....	141
Errors.....	146
Size.....	149
MAC Address.....	150
IGMP Snooping.....	152
Dynamic Group Registration.....	152
VLAN Status.....	152
Port Access Control.....	153
Maintenance.....	156
TFTP Services.....	156
Switch History.....	159
Ping Test.....	160
Save Changes.....	160
Factory Reset.....	161
Restart System.....	161
Connection Timeout.....	162
Logout.....	162
Help.....	162
Technical Specifications.....	163
RJ-45 Pin Specification.....	165
Runtime Switching Software Default Settings.....	166
Understanding and Troubleshooting the Spanning Tree Protocol.....	168
Blocking State.....	168
Listening State.....	168
Learning State.....	169
Forwarding State.....	170
Disabled State.....	171

Troubleshooting STP	172
Spanning Tree Protocol Failure.....	172
Full/Half Duplex Mismatch.....	173
Unidirectional Link	174
Packet Corruption.....	174
Resource Errors.....	174
Identifying a Data Loop	175
Avoiding Trouble.....	175
Brief Review of Bitwise Logical Operations	178
Index.....	179

ABOUT THIS GUIDE

This User's Guide tells you how to install your DES-3210/DES-3218/DES-3226, how to connect it to your Ethernet/Fast Ethernet/Gigabit Ethernet network, and how to set its configuration using the built-in console interface.

Overview of this User's Guide

Chapter 1, "*Introduction.*" Describes the Switch and its features.

Chapter 2, "*Unpacking and Setup.*" Helps you get started with the basic installation of the Switch.

Chapter 3, "*Identifying External Components.*" Describes the front panel, rear panel, optional plug-in modules, and LED indicators of the Switch.

Chapter 4, "*Connecting the Switch.*" Tells how you can connect the Switch to your Ethernet/Fast Ethernet/Gigabit Ethernet network.

Chapter 5, "*Switch Management and Operating Concepts.*" Talks about Local Console Management via the RS-232 DCE console port and other aspects about how to manage the Switch.

Chapter 6, "*Using the Console Interface.*" Tells how to use the built-in console interface to change, set, and monitor Switch performance and security.

Chapter 7, "*Web-Based Network Management.*" Tells how to manage the Switch through an Internet browser.

Appendix A, "*Technical Specifications.*" Lists the technical specifications of the Switch.

Appendix B, "*RJ-45 Pin Specifications.*" Shows the details and pin assignments for the RJ-45 receptacle/connector.

Appendix C, "Factory Default Settings."

Appendix D, "Understanding and Troubleshooting the Spanning Tree Protocol."

Appendix E, "Brief Review of Bitwise Logical Operations."

INTRODUCTION

This section describes the features of the DES-3210/DES-3218/DES-3226

Features

The Switch was designed for easy installation and high performance in an environment where traffic on the network and the number of users increases continuously.

Switch features include:

Ports

- Either 8, 16 or 24 high performance NWay (MDI-II/MDI-X) ports for connecting to end stations, servers and hubs. Every port can be used for an uplink connection and there are four priority queues per port.
- All UTP ports can auto-negotiate between 10Mbps/100Mbps, half-duplex or full duplex.
- One front panel slide-in module interface for a 2-port GBIC Module, 2-port 1000BASE-LX Module, 2-port 1000BASE-SX Module, 2-port 1000BASE-T Module, 1 and 2-port 100BASE-FX Modules, and 2-port 10/100BASE-TX Module.
- Fully compliant with IEEE 802.3 10BASE-T and IEEE 802.3u 100BASE-TX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-SX and IEEE 802.3u 100BASE-FX.
- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

Performance Features

- 8.8 Gbps switching fabric capacity
- Store and forward switching scheme.
- Full and half-duplex for both 10Mbps and 100Mbps connections. Full duplex allows the switch port to simultaneously transmit and receive data, and only works with connections to full-duplex capable end stations and switches. Connections to hubs must take place at half duplex.
- Broadcast Storm filtering.
- Port Mirroring support.
- Data forwarding rate 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data forwarding rate 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- Data forwarding rate 1,488,095 pps per port at 100% of wire-speed for 1000Mbps speed
- Data filtering rate eliminates all error packets, runts, etc. at 14,880 pps per port at 100% of wire-speed for 10Mbps speed.

- Data filtering rate eliminates all error packets, runts, etc. at 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 1,488,095 pps per port at 100% of wire-speed for 1000Mbps speed.
- 8K active MAC address entry table per device with automatic learning and aging (10 to 1000000 seconds).
- 8 MB packet buffer per device.
- Bandwidth control for all ports.
- Auto-Negotiation support for automatically selecting optimal transmission speed (10/100Mbps) and mode (Full/Half Duplex).
- Traffic Segmentation support.
- 802.1D Spanning Tree support and 802.1w Rapid Spanning Tree support.
- 802.1Q Tagged VLAN support, including GVRP (GARP VLAN Registration Protocol) support for automatic VLAN configuration distribution. All the supported VLANs (including dynamic joined VLANs by GVRP and user-defined VLANs and the one reserved VLAN) can be up to 255.
- GMRP support.
- IGMP Snooping support.
- Port trunking support.
- RADIUS client support.
- EAPOL support.

Management

- RS-232 console port for out-of-band network management via a console terminal, with authentication.
- Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops.
- Multiple access rights for different users.
- Built-in SNMP V.1/V.2C/V3 agent with management.
- Fully configurable either in-band or out-of-band control via SNMP based software.
- Flash memory for software upgrades. This can be done in-band via TFTP or out-of-band via the console.
- MIB support for:
 - D-Link MIB
 - MIB-II (RFC 1213)
 - Bridge MIB (RFC 1493)
 - Mini-RMON MIB (RFC 1757) – 4 groups. The RMON specification defines the Counters for the Receive functions only. However, the DHS-3226 implements counters for both receive and transmit functions.
 - IF-MIB (RFC 2233)
 - 802.1q MIB (RFC 2674)
 - Entity MIB (RFC 2737)
 - 802.1p MIB (RFC 2674)
 - Ether-Like MIB (RFC 2358) –dot3StatsTable
 - SNMP V.1 (RFC 1215), SNMP V.2-MIB (RFC 1907)
 - 802.1X MIB

- Enterprise MIB
 - Framework MIB (RFC 2571)
 - MDP MIB (RFC 2572)
 - Notify MIB (RFC 2573)
 - USM MIB (RFC 2574)
 - VACM MIB (RFC 2575)
 - Community MIB (RFC 2576)
 - Radius-Auth-Client MIB (RFC 2618)
 - SSH MIB
- Supports Web-based management.
 - TFTP support.
 - BOOTP support.
 - DHCP Client support.
 - RMON support.
 - Upgradeable firmware via TFTP or out-of-band via the console.
 - Backup and Restore Configuration files.
 - Password enabled.
 - Telnet remote control console support.
 - 802.1X port-based authentication support. Authentication methods: EAP MD5-Challenge (RFC 1994) and EAP TLS Authentication Protocol (RFC 2716).
 - Port Security for up to 10 MAC Addresses
 - Diffserv support
 - SSH Security Shell And TACACS support.

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-3210 8-port, DES-3218 16-port or DES-3226 24-port Fast Ethernet Switch
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This User's Guide with Registration Card

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

Installation

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

- The surface must support at least 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.

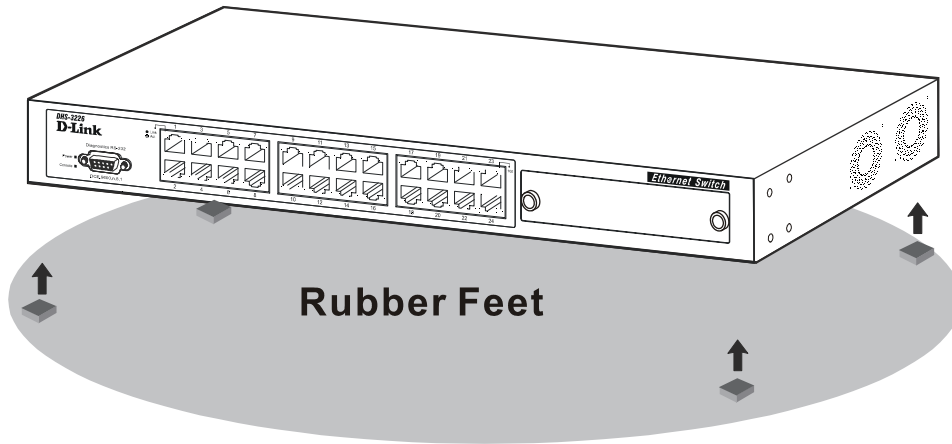


Figure 2-1. Installing rubber feet for desktop installation

Rack Installation

The DES-3210/DES-3218/DES-3226 can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

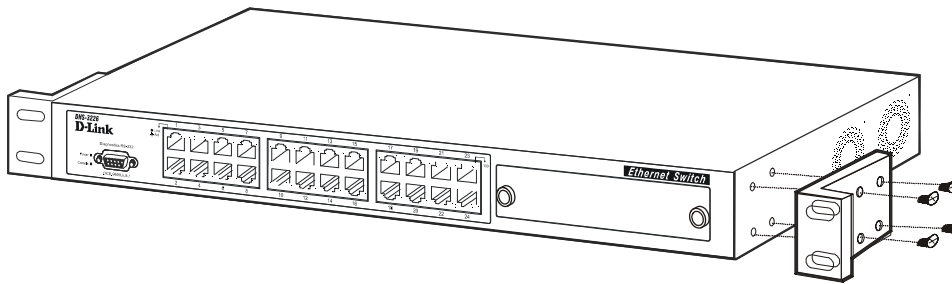


Figure 2- 2A. Attaching the mounting brackets to the Switch

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

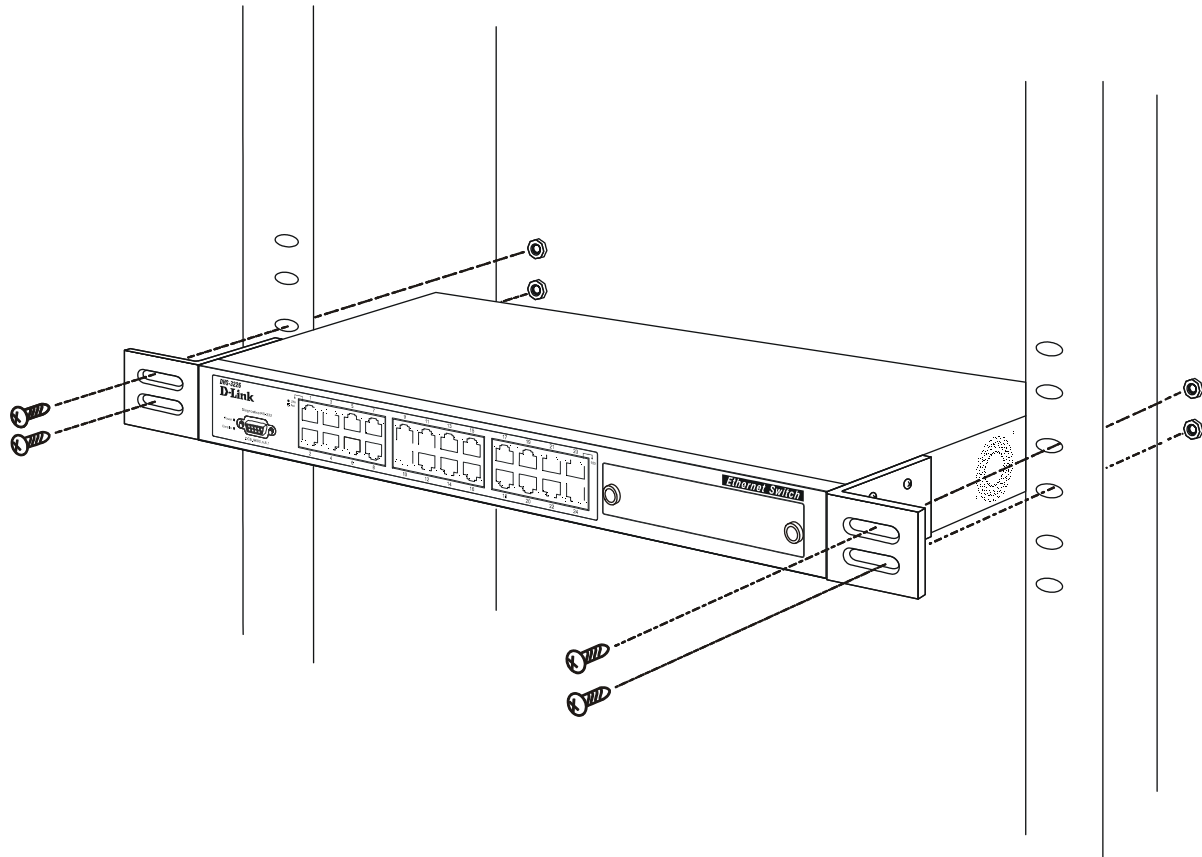


Figure 2-2B. Installing the Switch in an equipment rack

Power on

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

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

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

Power Failure

As a precaution in the event of a power failure, unplug the Switch. When power is resumed, plug the Switch back in.

3

IDENTIFYING EXTERNAL COMPONENTS

This chapter describes the front panel, rear panel, side panels, optional plug-in modules, and LED indicators of the DES-3210/DES-3218/DES-3226.

Front Panel

The front panel of the Switch consists of LED indicators, an RS-232 communication port, and 8, 16 or 24 MDI-X/MDI-II Ethernet/Fast Ethernet (10/100 Mbps) ports, each of which is capable of making an uplink connection.

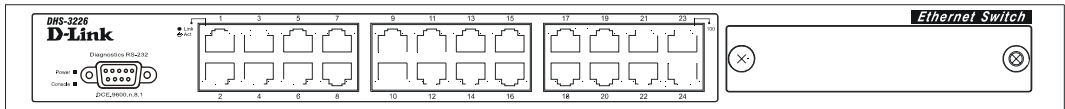


Figure 3-1. Front panel view of the Switch

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.

Eight (DES-3210), sixteen (DES-3218) or twenty-four (DES-3226) high-performance Nway Ethernet ports all of which operate at 10/100 Mbps for connections to end stations, servers and hubs. All ports can auto-negotiate between 10Mbps or 100Mbps and full or half duplex.

A front-panel slide-in module slot can accommodate a 1-port 100BASE-FX (2Km), 2-port 100BASE-FX (2Km), 1-port 100BASE-FL (15Km), 2-port 100BASE-FL (15Km), 2-port 1000BASE-SX, 2-port 1000BASE-LX, 2-port 1000BASE-T, or 2-port GBIC module to connect to another switch, server or network backbone.

Rear Panel

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

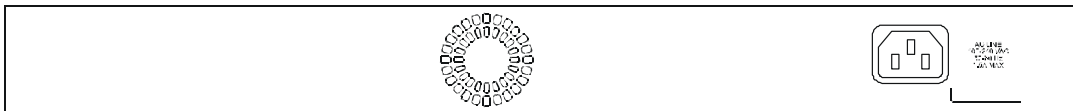


Figure 3-2. Rear panel view of the Switch

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.

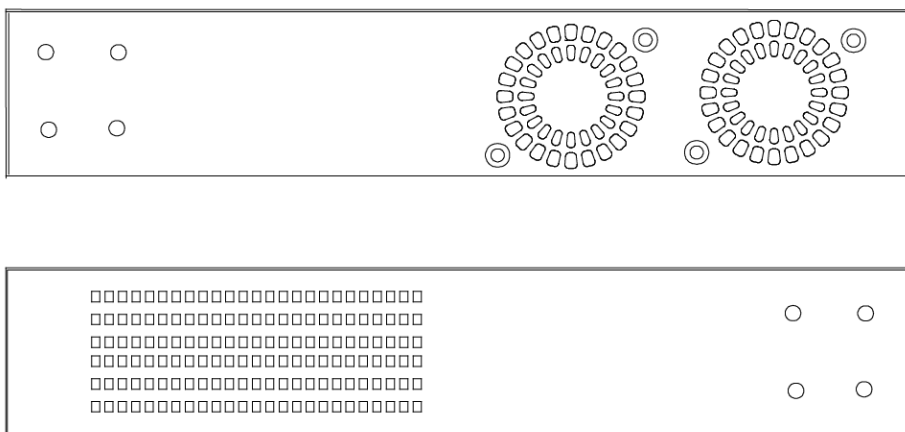


Figure 3-3. Side panel views of the Switch

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 100BASE and 1000BASE Extension Modules

The DES-3210, DES-3218 and the DES-3226 are able to accommodate a range of optional plug-in modules in order to increase functionality and performance. These modules must be purchased separately.

100BASE-FX Module (2Km)

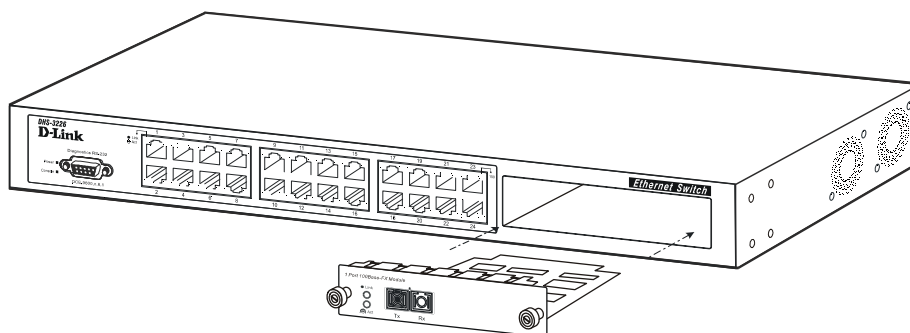


Figure 3-4. Optional 100BASE 1-port front panel module

- One 100BASE-FX (with SC type connector) Fiber port.
- Fully compliant with IEEE802.3u.
- Support Full-duplex operation only.
- IEEE 802.3x compliant Flow Control support for full duplex.

100BASE-FX Module (2Km)

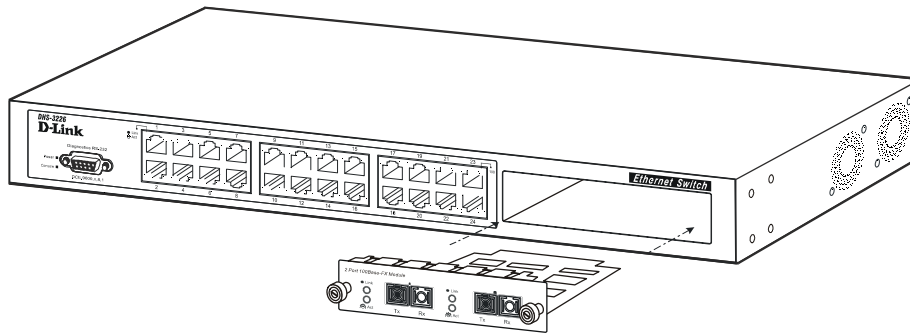


Figure 3-5. Optional 100BASE 2-port front panel module

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

1000BASE-LX Gigabit Module

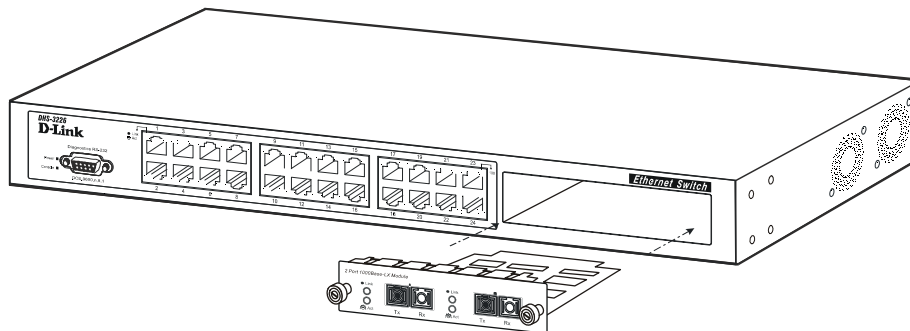


Figure 3-8. Optional 1000BASE-LX 2-port front panel module

Two 1000BASE-LX ports.
Connects to 1000BASE-LX devices at full duplex or auto.
Allows connections up to 5 km in length using single-mode fiber optic cable.

1000BASE-SX Gigabit Module

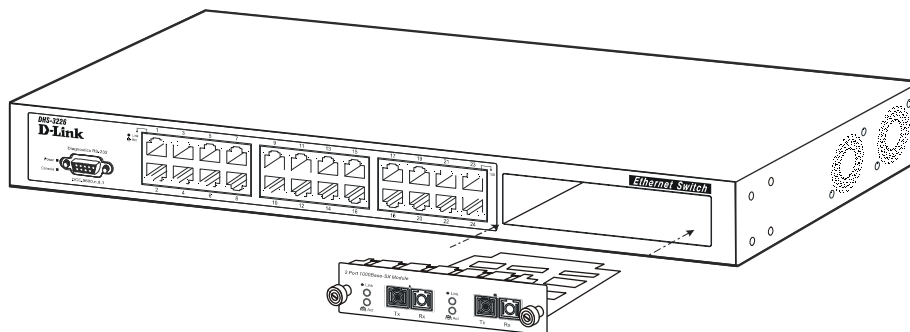


Figure 3-9. Optional 1000BASE-SX 2-port front panel module

Two 1000BASE-SX ports.

Connects to 1000BASE-SX devices at full duplex or auto.
 IEEE 802.3x compliant Flow Control support for full duplex.
 Supports multi-mode fiber-optic cable connections of up to 2 km.
 Allows connections using multi-mode fiber optic cable in the following configurations:

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

1000BASE-T Copper Gigabit Module

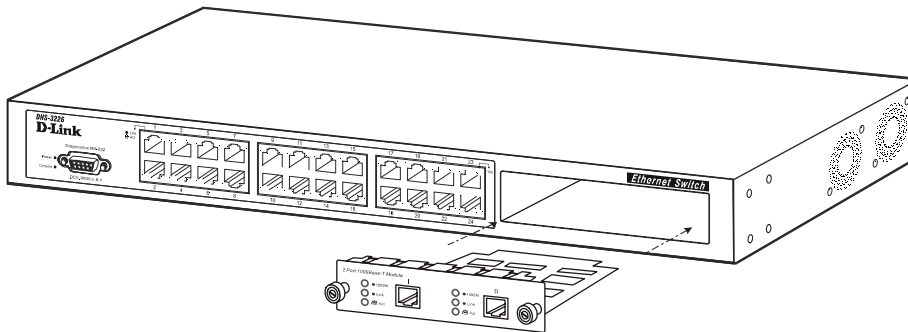


Figure 3-10. Optional 1000BASE-T Copper 2-port front panel module

Two 1000BASE-T Copper ports.
 Connects to 1000BASE-T devices at 1000M/full duplex, 100M/full duplex, 100M/half duplex, and Auto.
 Supports Category 5+ or higher cable connections of up to 100 meters.

1000BASE GBIC Module

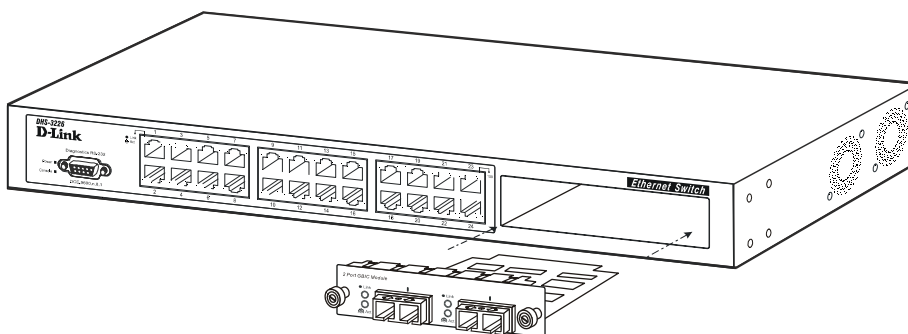


Figure 3-11. Optional 1000BASE GBIC 2-port front panel module

Two 1000BASE GBIC ports.
 Connects to GBIC devices at full duplex only.
 Allows multi-mode fiber optic cable runs of up to 550m in full-duplex mode (only).

LED Indicators

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

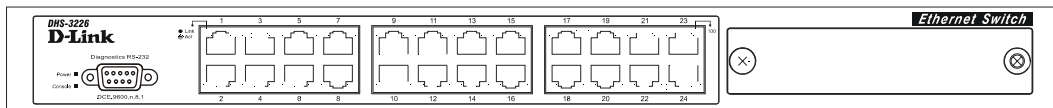


Figure 3-12. The LED indicators

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.

Speed – On the right of each twisted pair port, this LED will light when the corresponding port is operating at 100 Mbps. An unlit LED indicates a connection speed of 10 Mbps.

Link/Act – These indicators are located to the left of each port. They are lit when there is a secure connection (or link) to a device at any of the ports. The LEDs blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.

4

CONNECTING THE SWITCH

This chapter describes how to connect the DES-3210/DES-3218/DES-3226 to your Ethernet/Fast Ethernet/Gigabit Ethernet network.

Switch to End Node

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

An end node can be connected to the Switch via a two-pair Category 3, 4, or 5 UTP/STP cable. The end node should be connected to any of the ports of the Switch.

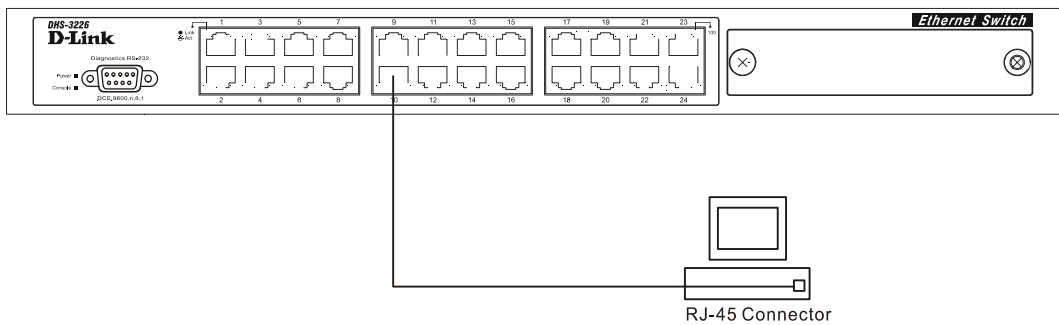


Figure 4-1. Switch connected to an End Node

The **Link/Act** LEDs for each UTP port light green when the link is valid. The LED on the right side of the port indicates port speed. It will light for 100 Mbps connections only. A blinking LED on the left side indicates packet activity on that port.

Switch to Hub or Switch

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

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

A 100BASE-TX hub or switch can be connected to the Switch via a two-pair Category 5 UTP/STP cable.

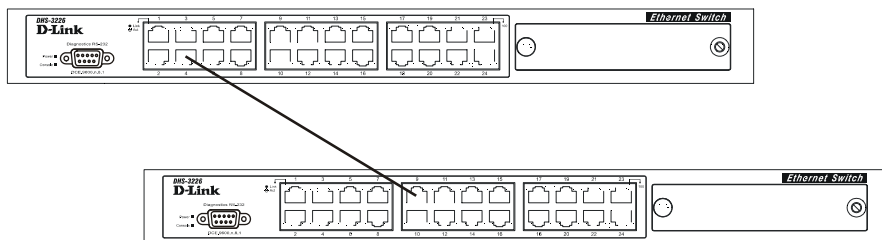


Figure 4-2. Switch connected to a normal (non-Uplink) port on a hub or switch using a straight or crossover cable

SWITCH MANAGEMENT AND OPERATING CONCEPTS

This chapter discusses many of the concepts and features used to manage the Switch, as well as the concepts necessary for the user to understand the functioning of the switch. Further, this chapter explains many important points regarding these features. Configuring the Switch to implement these concepts and make use of its many features is discussed in detail in the next chapters.

Local Console Management

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

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

The DES-3210/DES-3218/DES-3226 contains a CPU, memory for data storage, flash memory for configuration data, operational programs, and SNMP agent firmware. These components allow the Switch to be actively managed and monitored from either the console port or the network itself (out-of-band, or in-band).

Diagnostic (console) port (RS-232 DCE)

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

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

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

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

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

IP Addresses and SNMP Community Names

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

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

```

Boot Procedure 0.00.001
-----
Power On Self Test ..... 100 %

MAC Address   : 00-01-02-03-04-00
H/W Version   :

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

Figure 5-1. Boot Procedure screen

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

```

Switch Information
-----
Device Type       : D-Link DES-3226 Ethernet Switch
Ext.Module Type   : None
MAC Address       : 00-10-27-32-26-B1
Boot PROM Version : 1.00.003
Firmware Version  : 6.00.111
Base Module Version: 2B1
Ext.Module Version :

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

                APPLY
ADVANCED SETTINGS

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

Figure 5-2. Switch Information menu

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

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

Traps

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

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

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

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

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

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

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-user.

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

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

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

SNMP

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

SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol.
- Collecting information about the status and current configuration of network devices.
- Modifying the configuration of network devices.

The DES-3210/DES-3218/DES-3226 have a software program called an 'agent' that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

Authentication

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

Packet Forwarding

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

MAC Address Aging Time

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

The aging time can be from 10 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.

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

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

Some filtering is done automatically by the Switch:

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

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 source, destination, or both.

Spanning Tree Protocol

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

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

The DES-3210/DES-3218/DES-3226 STP allows two levels of spanning trees to be configured. The first level constructs a spanning tree on the links between switches. This is referred to as the **Switch** or **Global** level. The second level is on a port basis. Ports are configured as individual members of a spanning tree and the algorithm and protocol are applied to the specified ports. This is referred to as the **Port** level.

The Switch STP performs the following functions:

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

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

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

On the port level, STP sets the Root Port and the Designated Ports.

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

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

Table 5-1. STP Parameters – Switch Level

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

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	32768
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path.	100 – 100Mbps Fast Ethernet ports

Table 5-2. STP Parameters – Port Group Level

Bridge Protocol Data Units

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

- The unique switch identifier

- The path cost to the root associated with each switch port
- The port identifier
- STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:
 - The unique identifier of the switch that the transmitting switch currently believes is the root switch
 - The path cost to the root from the transmitting port
 - The port identifier of the transmitting port
- The Switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, rather the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.
- The communication between switches via BPDUs results in the following:
 - One switch is elected as the root switch
 - The shortest distance to the root switch is calculated for each switch
 - A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
 - A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
 - Ports included in the STP are selected.

Creating a Stable STP Topology

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

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

STP Port States

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

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

- Blocking – the port is blocked from forwarding or receiving packets
- Listening – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- Learning – the port is adding addresses to its forwarding database, but not yet forwarding packets
- Forwarding – the port is forwarding packets
- Disabled – the port only responds to network management messages and must return to the blocking state first
- A port transitions from one state to another as follows:
 - From initialization (switch boot) to blocking
 - From blocking to listening or to disabled
 - From listening to learning or to disabled

- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

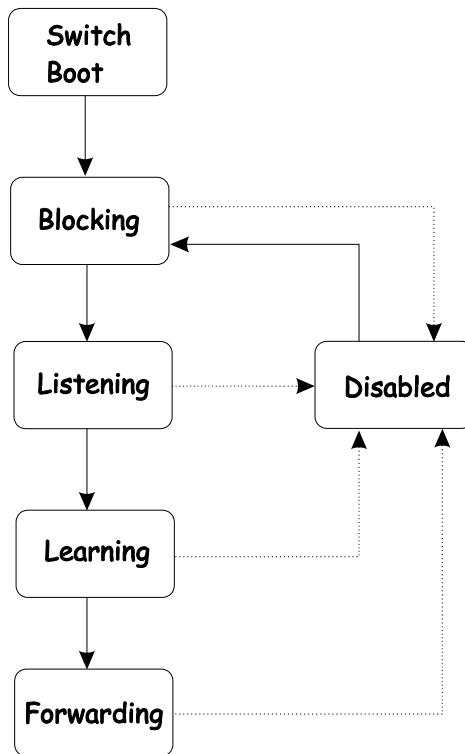


Figure 5-3. STP Port State Transitions

When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP enabled for all ports
Port priority	128
Port cost	100
Bridge Priority	32,768

Table 5-3. Default STP Parameters

User-Changeable STP Parameters

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

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

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

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

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

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

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

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

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

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

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

Illustration of STP

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

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

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

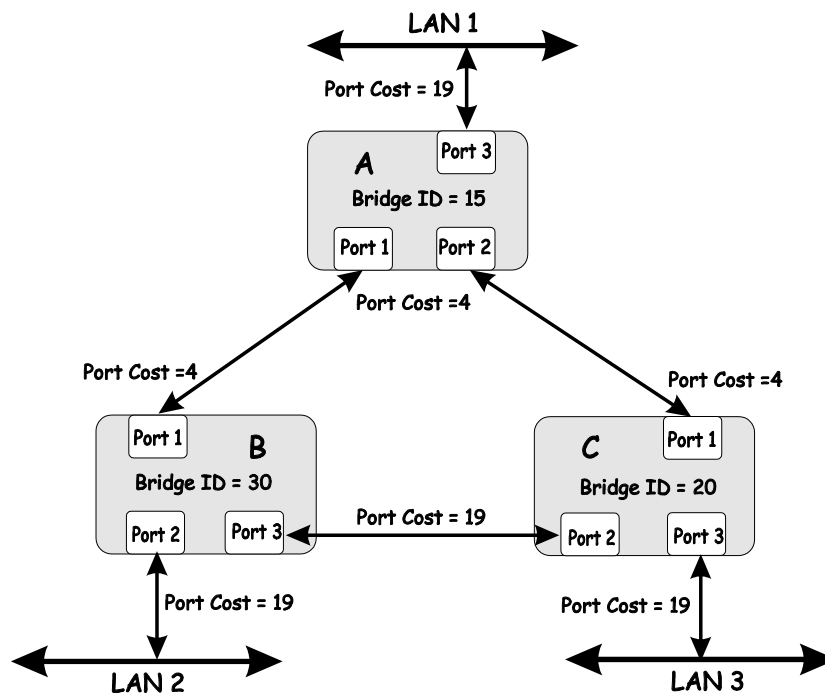


Figure 5-4. Before Applying the STA Rules

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

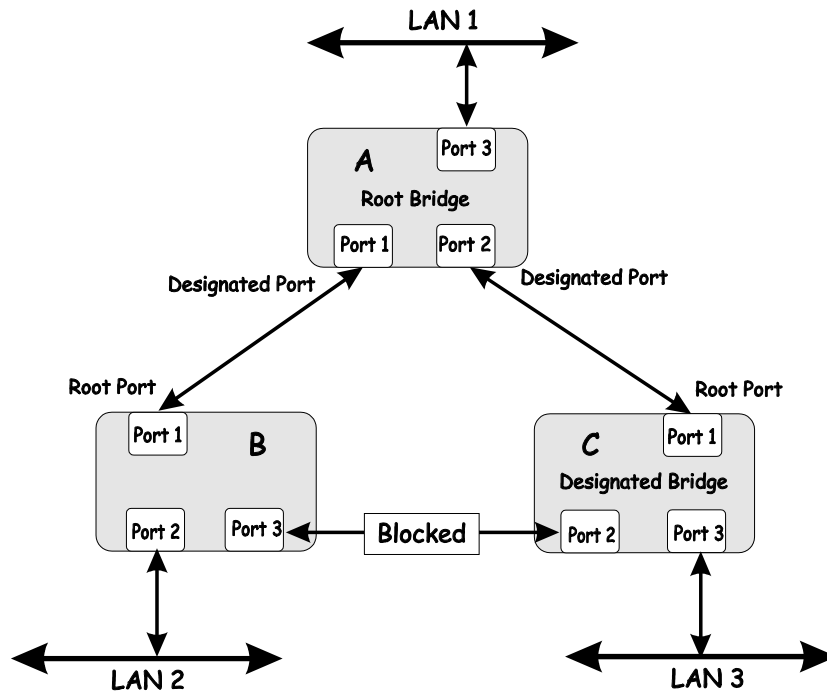


Figure 5-5. After Applying the STA Rules

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

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

VLANs

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

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

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

Notes About VLANs on the DES-3210/DES-3218/DES-3226

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets **cannot** cross VLANs without a network device performing a routing function between the VLANs.

The DES-3210/DES-3218/DES-3226 supports only IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN.

The DEFAULT_VLAN has a VID = 1.

The DES-3210/DES-3218/DES-3226 supports Asymmetric VLANs. The member ports of VLANs can be overlapped.

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-3210/DES-3218/DES-3226. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

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

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

Any port can be configured as either *tagging* or *untagging*. The *untagging* feature of IEEE 802.1Q VLANs 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-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

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

The main characteristics of IEEE 802.1Q are as follows:

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

802.1Q VLAN Packet Forwarding

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

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

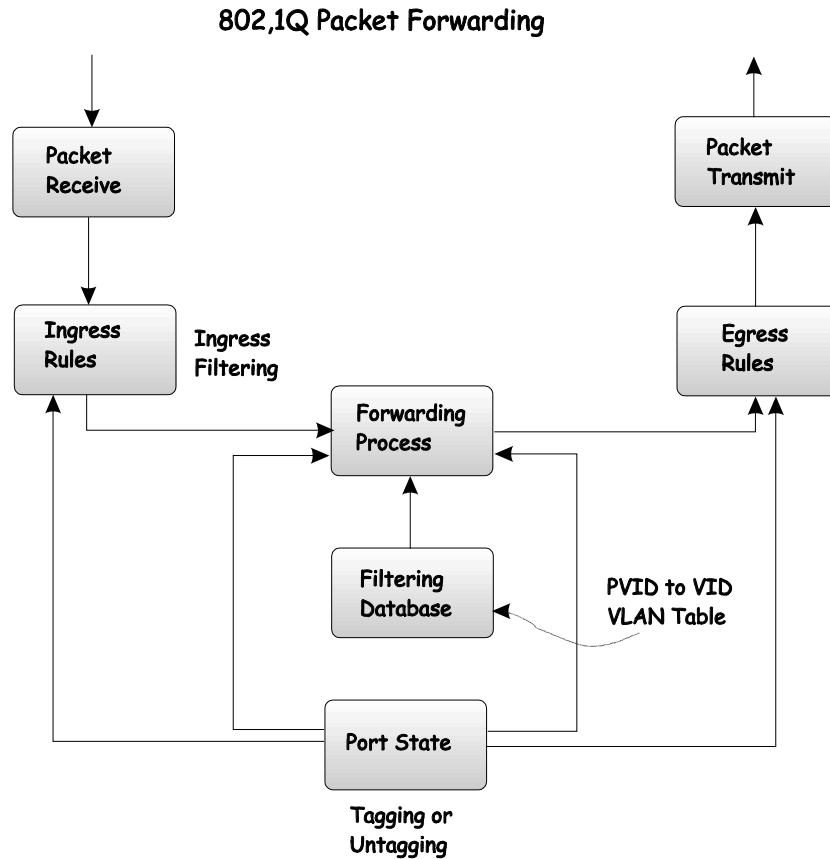


Figure 5-6. IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

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

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

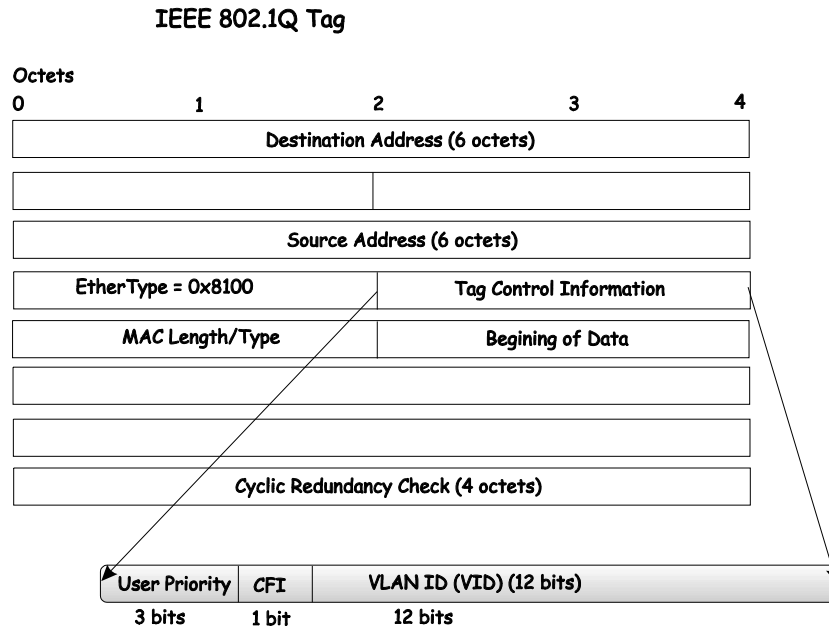


Figure 5-7. IEEE 802.1Q Tag

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.

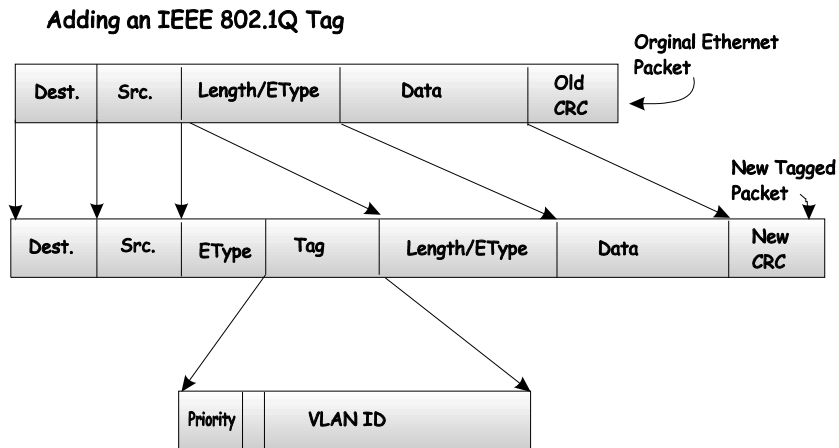


Figure 5-8. Adding an IEEE 802.1Q Tag

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.

VLANs

The Switch initially configures one VLAN, VID = 1, called the DEFAULT_VLAN. The factory default setting assigns all ports on the Switch to the DEFAULT_VLAN. As new VLANs are configured, their respective member ports are removed from the DEFAULT_VLAN.

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

Note: If no VLANs are configured on the switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

Note: Each IP interface on the Switch corresponds to a VLAN. The VLAN must be configured before the IP interface can be setup. The IP interface must have the same name (and the same VID number) as its corresponding VLAN.

The Switch allows ranges of IP addresses to be assigned to VLANs. Each VLAN must be configured prior to setting up the corresponding IP interface. An IP addressing scheme must then be established, and implemented when the IP interfaces are set up on the Switch.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Table 5-4. VLAN Example – Assigned Ports

In this case, 5 IP interfaces (or 5 subnets) are required, so a CIDR notation of 10.32.0.0/3 (or a 3-bit) addressing scheme will work. This addressing scheme will give a subnet mask of 11111111.11100000.00000000.00000000 (binary) or 255.224.0.0 (decimal).

Using a 10.xxx.xxx.xxx IP address notation would give 5 network addresses:

VLAN Name	VID	Network Address
System (default)	1	10.32.0.0
Engineering	2	10.64.0.0
Marketing	3	10.96.0.0
Finance	4	10.128.0.0
Sales	5	10.160.0.0

Table 5-5. VLAN Example – Assigned Network Addresses

Note: IP interfaces consist of two parts – a subnet mask and a network address.

Note: Each IP interface listed above will give a maximum of 2,080,800 unique IP addresses per interface (assuming the 10.xxx.xxx.xxx notation).

DHCP

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

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

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

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

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

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

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

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

802.1X Port-based Network Access Control

The Switch is an implementation of the server side of IEEE 802.1X-Port Based Network Access Control. Through this mechanism, users have to be authorized before being able to access the network. See the following figure:

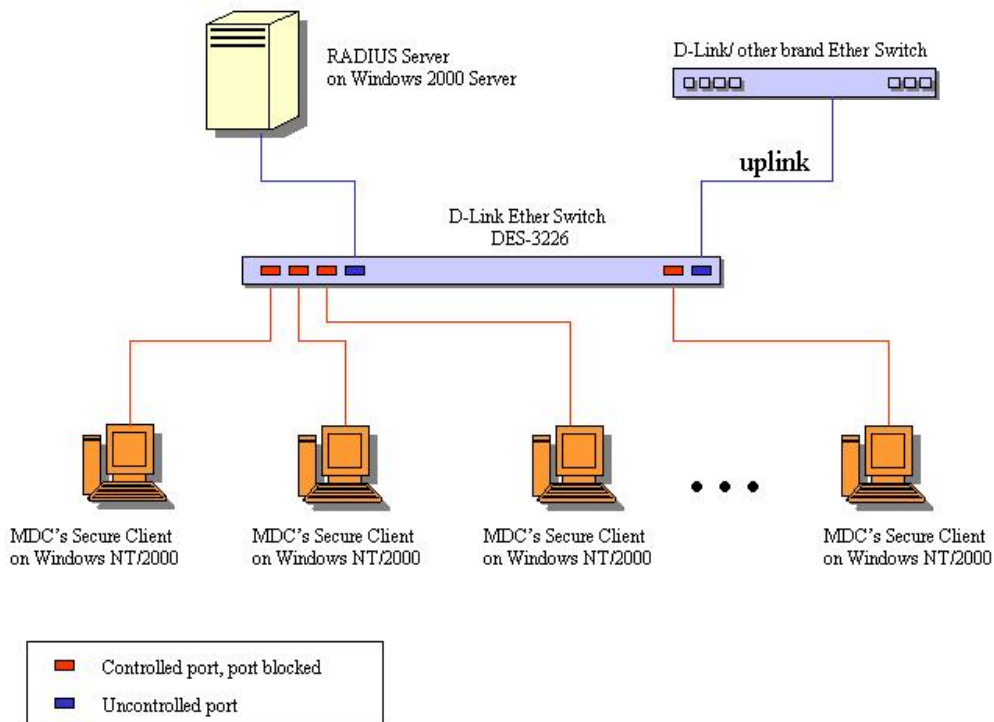


Figure 5-9. Typical 802.1X Configuration Prior to User Authentication

Once the user is authenticated, the switch unblocks the port that is connected to the user as shown in the next figure.

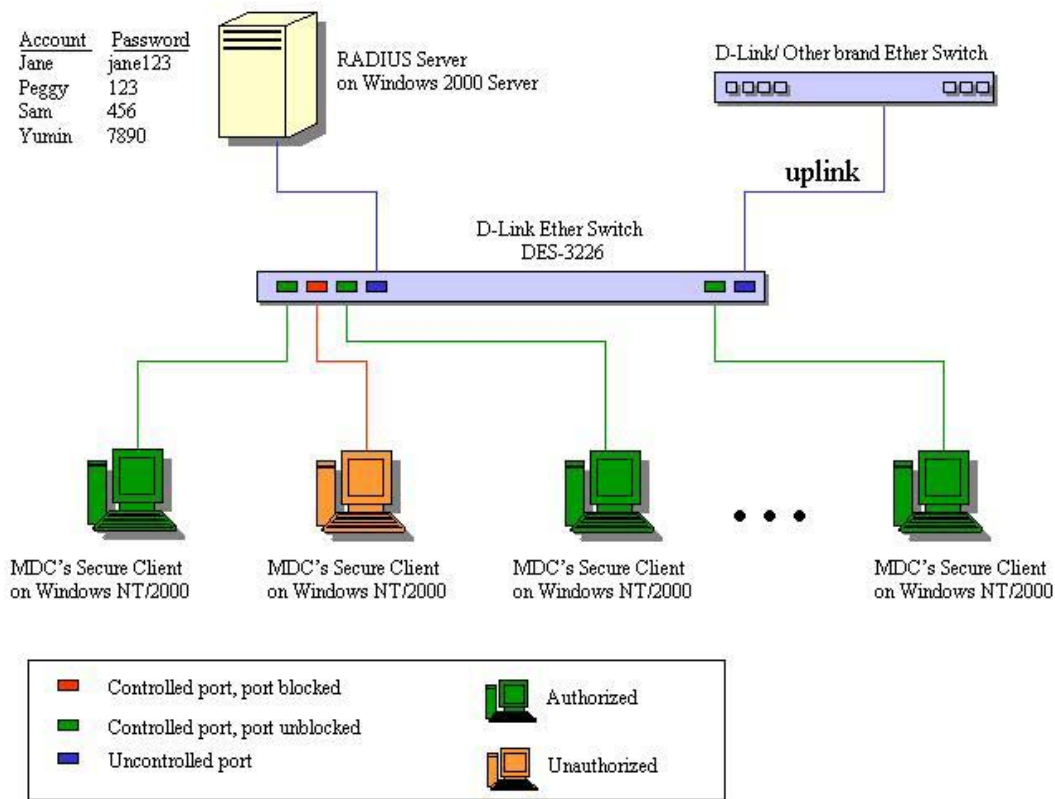


Figure 5-10. Typical 802.1X Configuration with User Authentication

The user's information, including account number, password, and configuration details such as IP address and billing information, is stored in a centralized RADIUS server.

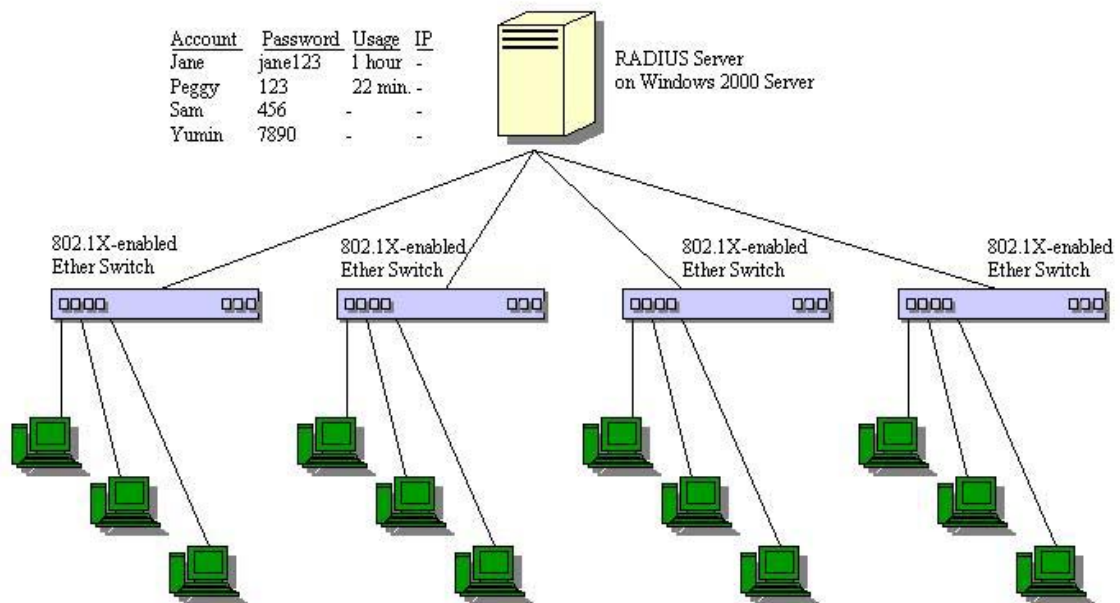


Figure 5-11. Typical Configuration with 802.1X Fully Implemented

State Machine Name
Port Timers state machine
Authenticator PAE state machine
The Authenticator Key Transmit state machine
Reauthentication Timer state machine
Backend Authentication state machine
Controlled Directions state machine
The Key Receive state machine

Table 5-6. Conformance to IEEE 802.1X Standards

CONFIGURING THE SWITCH USING THE CONSOLE INTERFACE

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

Notes are added where clarification is necessary.

Before You Start

The DES-3210/DES-3218/DES-3226 supports a wide array of functions and gives great flexibility and increased network performance by eliminating the routing bottleneck between the WAN or Internet and the Intranet. Its function in a network can be thought of as a new generation of router that performs routing functions in hardware, rather than software.

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

Connecting to the Switch

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

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

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

Console Usage Conventions

The console interface makes use of the following conventions:

- Items in *<angle brackets>* can be toggled between several choices using the space bar.

- Items in *[square brackets]* can be changed by typing in a new value. You can use the backspace and delete keys to erase characters behind and in front of the cursor.
- The up and down arrow keys, the left and right arrow keys, the tab key and the backspace key, can be used to move between selected items.
- Items in **UPPERCASE** are commands. Moving the selection to a command and pressing Enter will execute that command, e.g. APPLY, etc.

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

First Time Connecting to The Switch

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

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

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

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

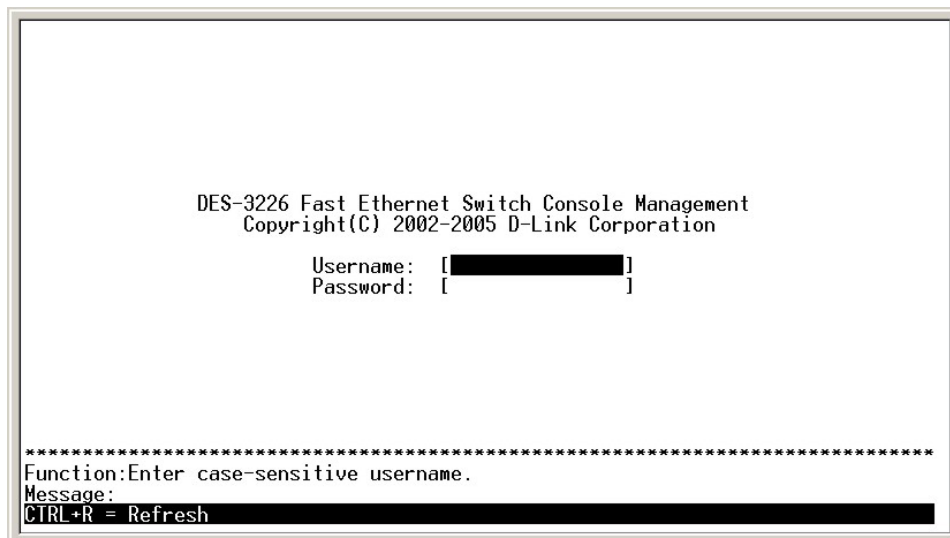


Figure 6-1. Initial screen, first time connecting to the Switch

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

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

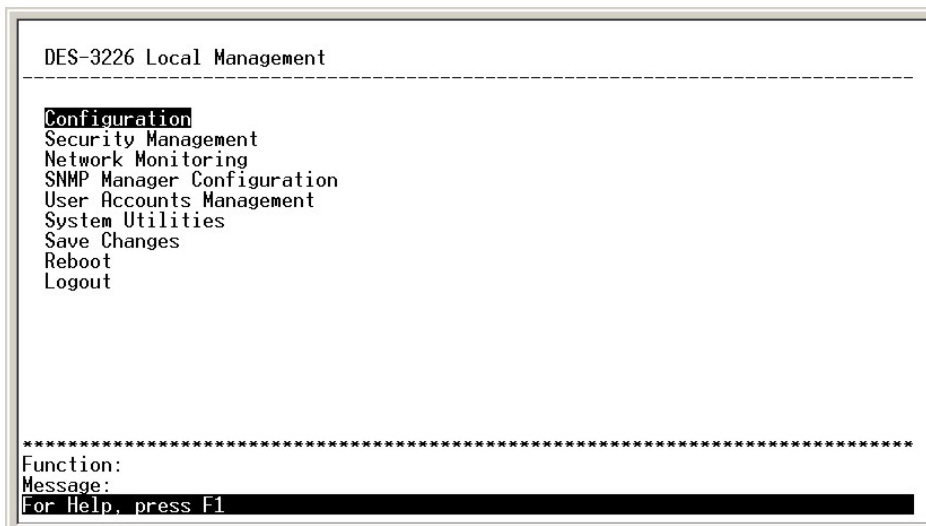


Figure 6-2. Main menu

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

User Accounts Management

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

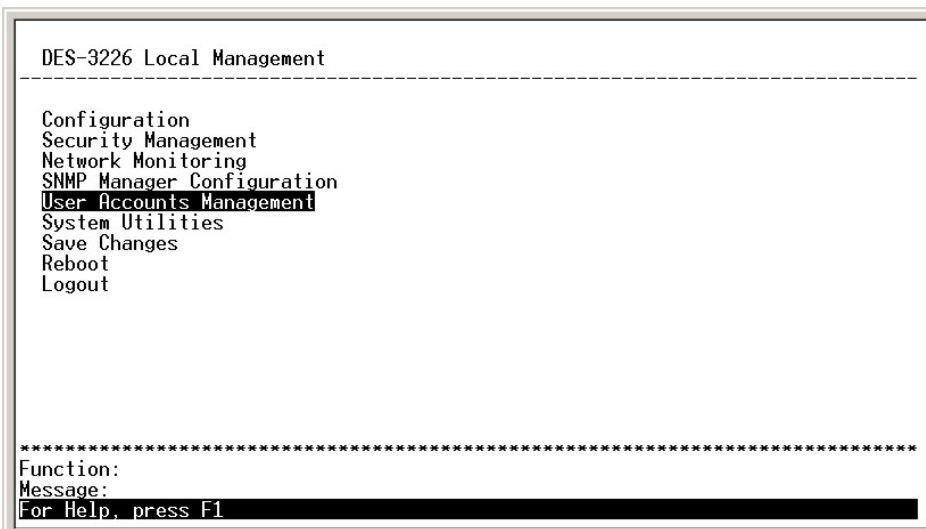


Figure 6-3. Main menu

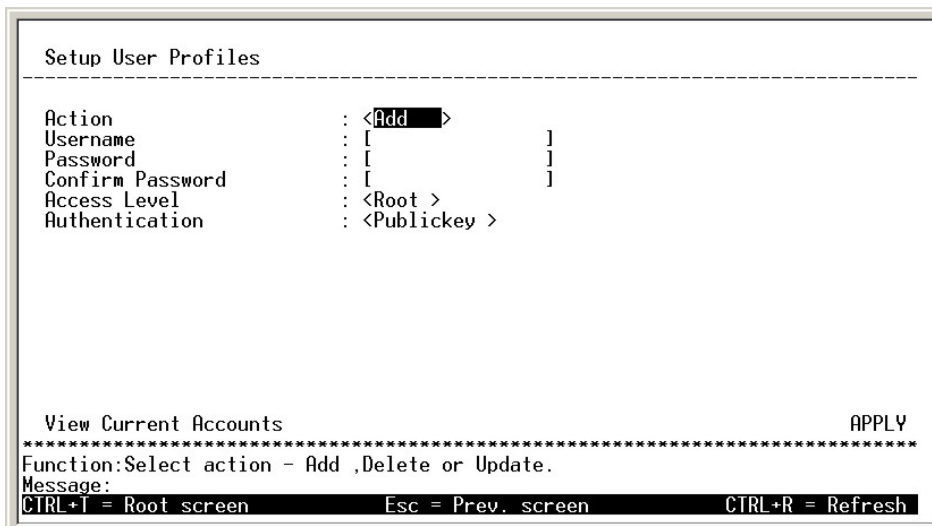


Figure 6-4. Setup User Profiles

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

Toggle the **Action** field to *Add* using the space bar. This will allow the addition of a new user. The other options are *Delete* - this allows the deletion of a user entry, and *Update* - this allows for changes to be made to an existing user entry.

Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have *Root*, *User+*, or *User* privileges. The space bar toggles between the three options.

Highlight **APPLY** and press **Enter** to make the user addition effective.

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

A listing of all user accounts and access levels is shown below the user setup menu. This list is updated when **APPLY** is executed.

Please remember that **APPLY** makes changes to the switch configuration for the *current session only*. All changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the main menu - if you want these changes to be permanent.

Root, User+ and Normal User Privileges

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

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

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

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

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

Save Changes

The DES-3210/DES-3218/DES-3226 has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by highlighting **APPLY** and pressing **Enter**. When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

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

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

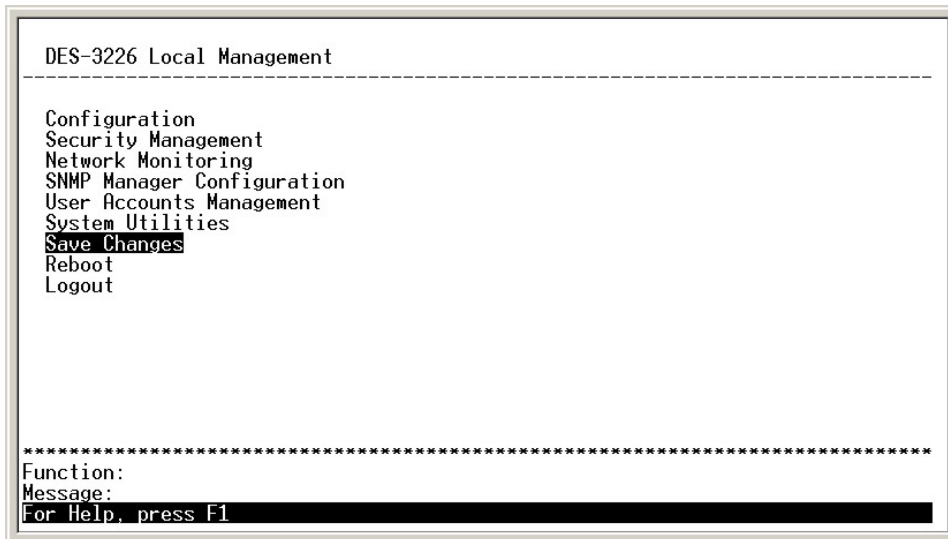


Figure 6-5. Main menu

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

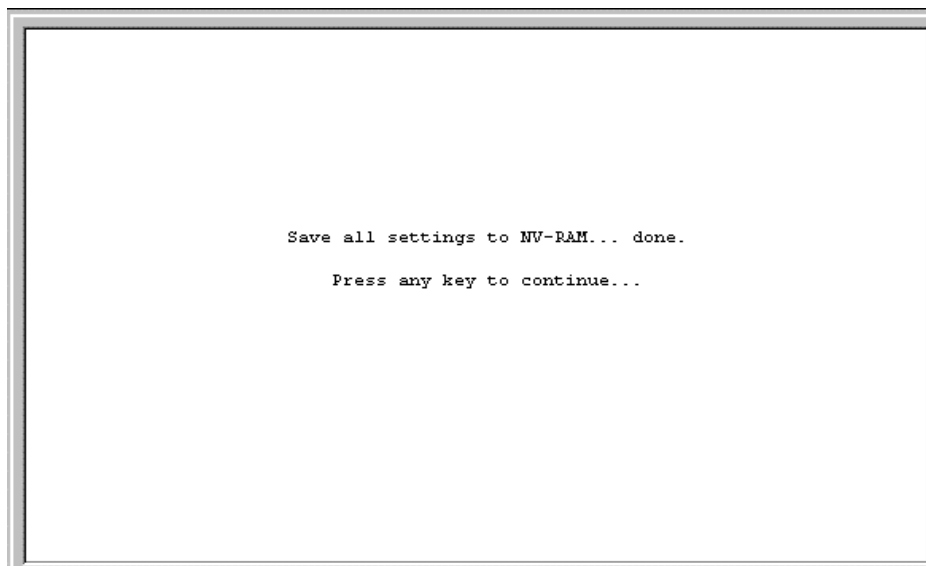


Figure 6-6. Save changes screen

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

Factory Reset

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

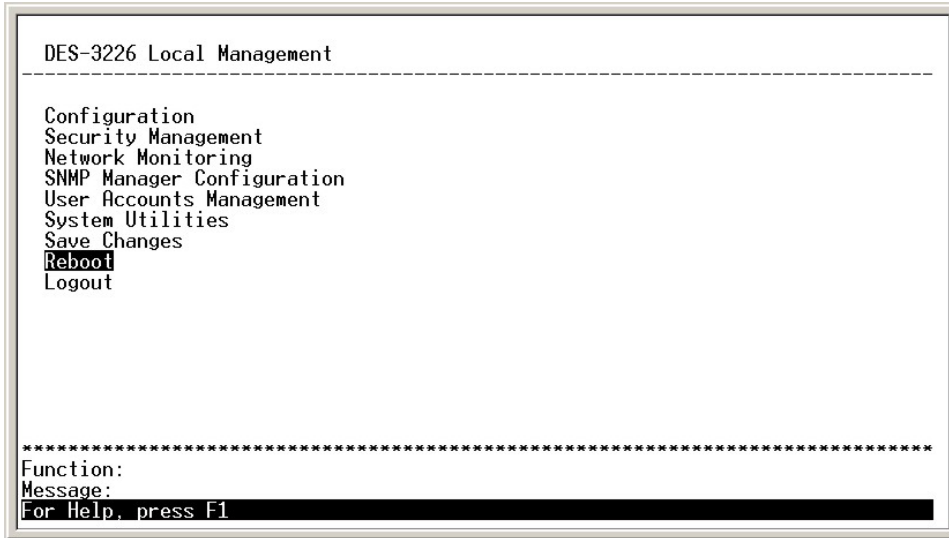


Figure 6-7. Main menu

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

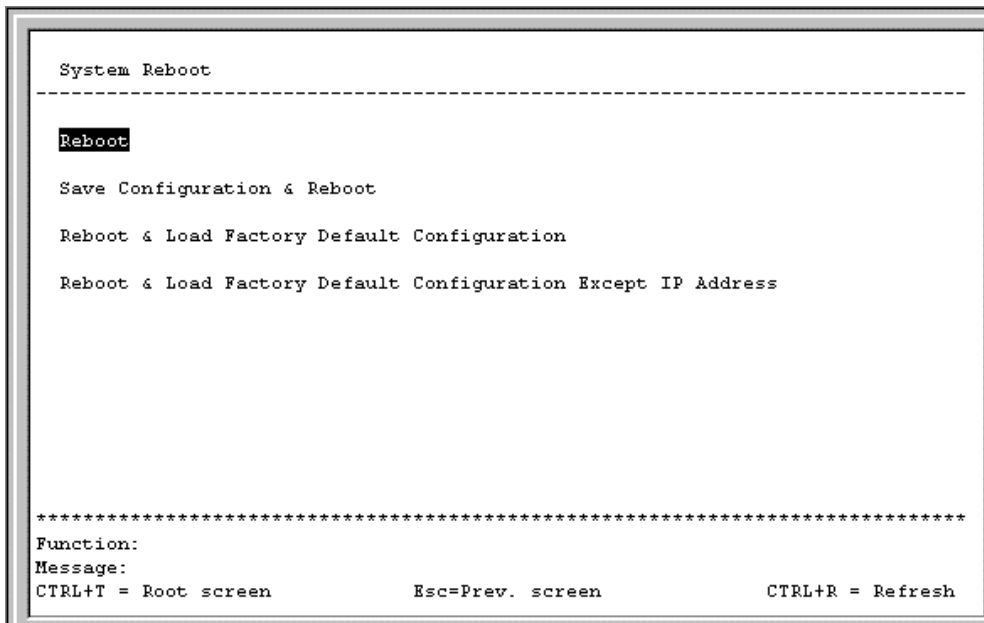


Figure 6-8. System Reboot menu

Highlight the appropriate choice and press **Enter** to reset the Switch's NV-RAM to the factory default settings (or just reboot the Switch). Loading the Factory Default Configuration will erase any User Accounts (and all other configuration settings) you may have entered and return the Switch to the state it was in when it was purchased. The **Load Factory Default Configuration Except IP Address** option is used when the Switch will be managed by the Telnet manager, which requires knowledge of the Switch's IP address to function.

Logging Onto The Switch Console

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

- Type in your **Username** and press **Enter**.
- Type in your **Password** and press **Enter**.

The main menu screen will be displayed based on your access level or privilege.

Updating or Deleting User Accounts

To update or delete a user password:

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

```

Setup User Profiles
-----
Action          : <Add >
Username        : [          ]
Password        : [          ]
Confirm Password : [          ]
Access Level    : <Root >
Authentication  : <Publickey >

View Current Accounts APPLY
*****
Function:Select action - Add ,Delete or Update.
Message:
CTRL+I = Root screen      Esc = Prev. screen      CTRL+R = Refresh
  
```

Figure 6-9. Setup User Accounts screen

Toggle the **Action** field using the space bar to choose *Add*, *Update*, or *Delete*.

Type in the **Username** for the user account you wish to change and enter the **Old Password** for that user account.

You can now modify the password or the privilege level for this user account.

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

If the privilege level is to be changed, toggle the **Access Level** field until the appropriate level is displayed – *Root*, *User+* or *User*.

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

You must enter the configuration changes into the non-volatile ram (NV-RAM) using **Save Changes** from the main menu if you want the configuration to be used after a switch reboot.

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

Viewing Current User Accounts

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

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

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

Deleting a User Account

Toggle the **Action** field to **Delete**.

Enter the **Username** and **Old Password** for the account you want to delete. You must enter the password for the account to be able to delete it.

Highlight **APPLY** and press **Enter** to make the deletion of the selected user take effect.

You must enter the configuration changes into the non-volatile ram (NV-RAM) using **Save Changes** from the main menu if you want the configuration to be used after a switch reboot.

Only users with **Root** privileges can delete user accounts.

Configuration

This section will help prepare the Switch user by describing the Remote Management Setup, Switch Information, Configure Advanced Switch Features, Configure Ports, Bandwidth Configuration, Configure Spanning Tree, Port Spanning Tree Settings, Setup Unicast Filtering Table, Setup Static Multicast Filtering Table, IEEE 802.1Q VLANs Configuration, 802.1Q Static VLAN Settings, Port VLAN assignment, Ingress Filter Settings, Port GVRP Settings, IGMP Snooping Settings, Port LACP Trunking Settings, Setup Port Mirroring, Setup Threshold of Broadcast/Multicast/DA-Unknown Storm, Port Security Settings, Configure Class of Service, Default Priority and Traffic Class, Port GMRP Settings, Diffserv Settings, and PAE Configuration screens, all of which can be found under the Configuration menu, along with various submenus.

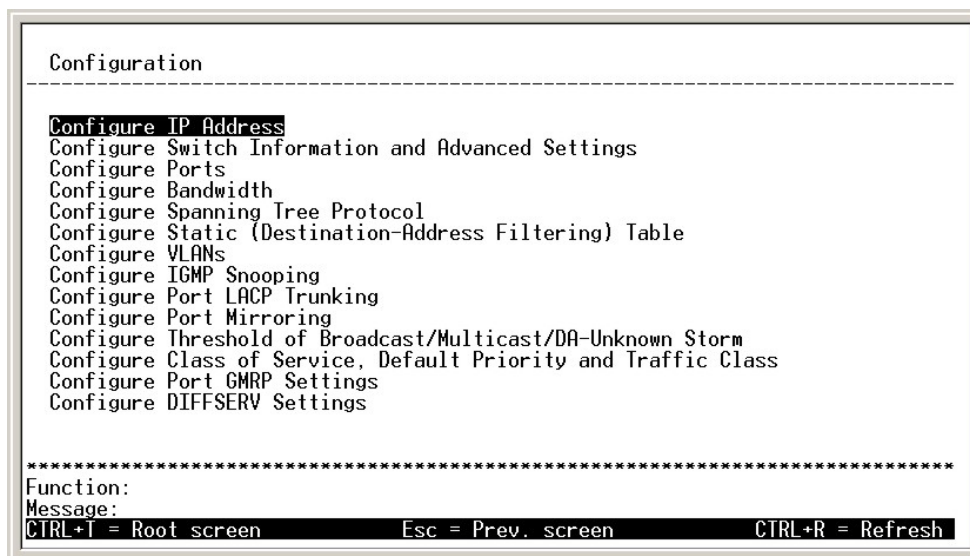


Figure 6-10. Configuration menu

Configure IP Address

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

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

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


```

Remote Management Setup
-----

Current Switch IP Settings:

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

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

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

```

Figure 6-11. Remote Management Setup screen

The Switch needs to have an IP address assigned to it so that an In-Band network management system (e.g. Telnet) client can find it on the network. The **Remote Management Setup** screen allows you to change the settings for the two different management interfaces used on the Switch: the Ethernet interface used for in-band communication, and the SLIP interface used over the console port for out-of-band communication.

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

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

The **Get IP From** options are:

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

DCHP – The Switch will send out a DCHP broadcast request when it is powered up. The DCHP protocol allows IP addresses, network masks, and default gateways to be assigned by a DCHP server. If this option is set, the switch will first look for a DCHP 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 that 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.
- **Management VID** – Allows the entry of the VLAN ID (VID) of a VLAN that will have access to the Telnet manager. This will be the VID of the VLAN that a management station is located on.

Configure Switch Information and Advanced Settings

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

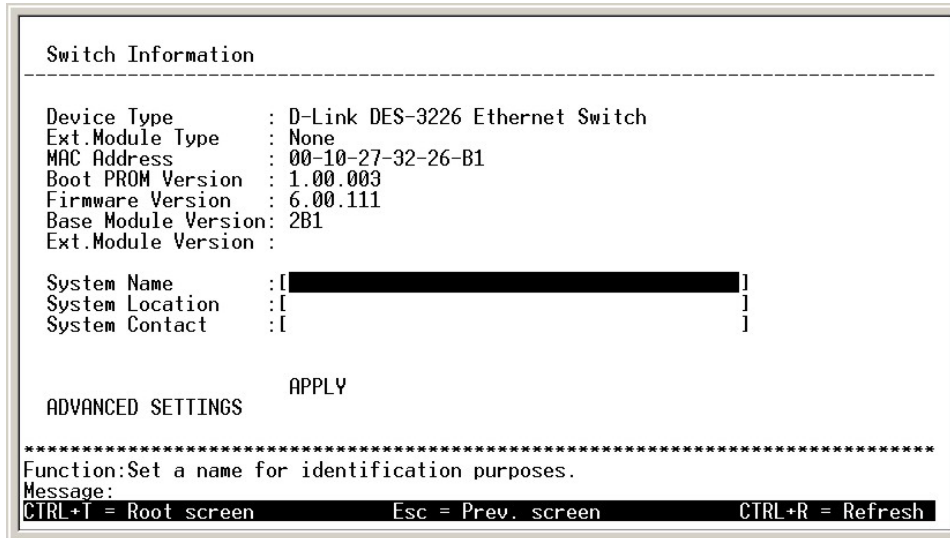


Figure 6-12. Switch Information menu

The **Switch Information** menu shows the type of switch, 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.

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

Configure Advanced Switch Features

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

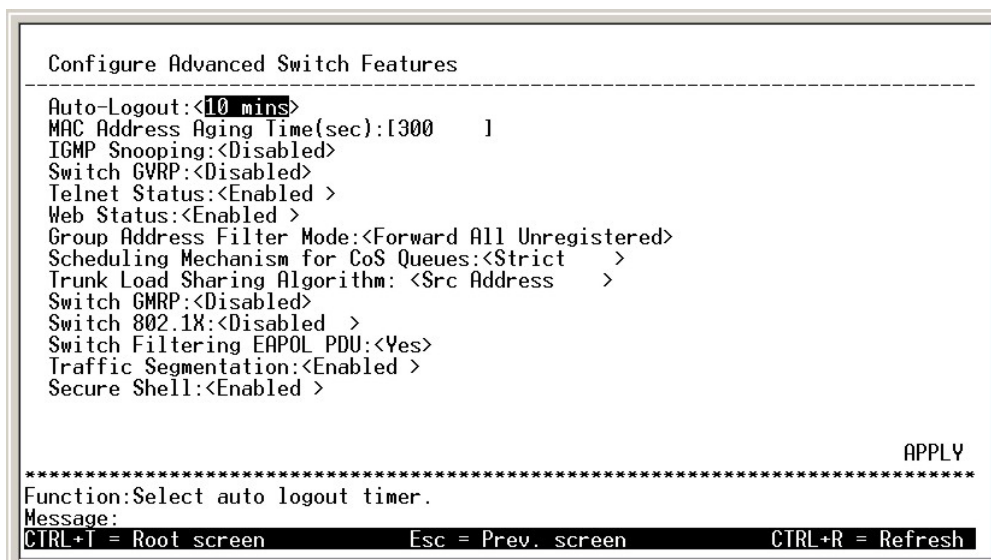


Figure 6-13. Configure Advanced Switch Features screen

This screen allows you to set the following features:

Auto-Logout:<10 mins> – This sets the time the interface can be idle before the Switch automatically logs-out the user. The options are *2 mins*, *5 mins*, *10 mins*, *15 mins*, or *Never*.

MAC Address Aging Time (sec):[300] – This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between 10 and 1,000,000 seconds.

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

IGMP Snooping:<Disabled> – This setting enables Internet Group Management Protocol (IGMP) Snooping, which enables the Switch to read IGMP packets being forwarded through the Switch in order to obtain forwarding information from them (learn which ports contain Multicast members).

Switch GVRP:<Disabled> – Group VLAN Registration Protocol is a protocol that allows members to dynamically join VLANs. This is used to enable or disable GVRP on the Switch

Telnet Status:<Enabled> – Toggle to *Enabled* to allow access to the Switch over the network using the TCP/IP Telnet protocol.

Web Status:<Enabled> – You can also use a Web-based browser to manage the Switch by toggling to *Enabled*.

Group Address Filter Mode:<Forward All Unregistered> – The IGMP filter mode for processing multicast packets. The options are *Forward All*, *Forward All Unregistered*, and *Filtered All Unregistered*.

Scheduling Mechanism for CoS Queues:<Strict> – There are two Class of Service queue options, *RoundRobin* and *Strict*. If *Strict* is selected, when the highest priority queue is full, those packets will be the first to be forwarded. If *RoundRobin* is selected, the forwarding is based on the settings made on the **Class of Service Configuration** screen.

Trunk Load Sharing Algorithm:<Src Address> – The trunk load sharing options are *Dst Address*, *Src&Dst Address*, and *Src Address*.

Switch GMRP:<Disabled> – Group Multicast Registration Protocol is a protocol that allows members to dynamically join Multicast groups. GMRP must also be enabled on specific ports on the **Port GMRP Settings** screen for it to take effect. This global control is especially useful if you want to turn off GMRP on the whole Switch without making changes to each individual port.

Switch 802.1X:<Disabled> – Set the 802.1X access control by toggling between *Disabled*, *Port-Based* and *MAC-Based*.

Switch Filtering EAPOL PDU:<Yes> – This option is only available if 802.1X is disabled. It filters Extensible Authentication Protocol Over LANs Packet Data Units (EAPOL PDU) when enabled.

Switch Traffic Segmentation:<Disabled> – When this feature is *Enabled*, ports on the Switch are not able to communicate with one another except server port(s). If there is not an optional module present, Port 1 becomes the server port. If there is a 1-port optional module, this port will be the server port. If there is a 2-port optional module, both ports act as server ports.

Secure Shell:<Enabled> – When this feature is *Enabled*, the switch encrypts all transmitted data for secure remote access over IP networks.

Configure Ports

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

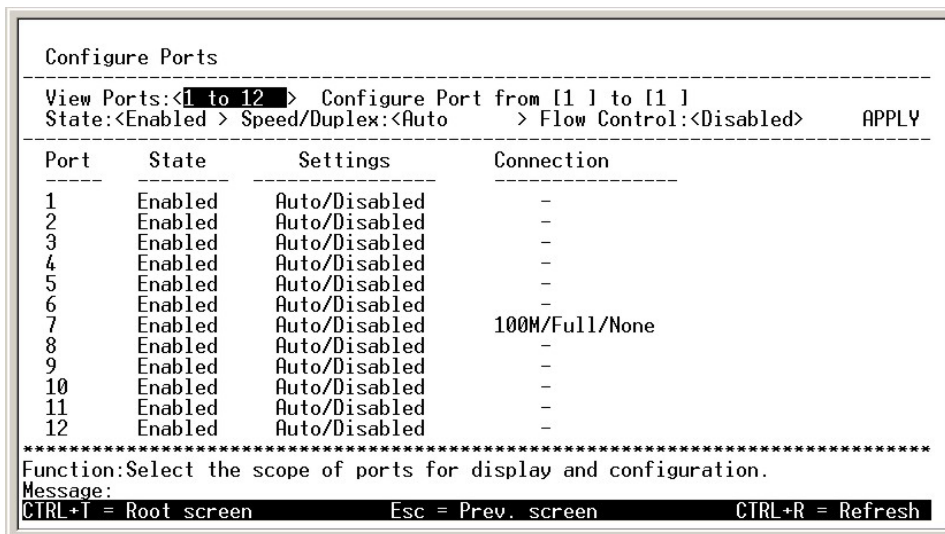


Figure 6-14. Configure Ports screen

Toggle the **View Ports** field, using the space bar, to view the configuration of either ports 1 through 8 or ports 9 through 16. To configure a specific port, toggle the **Configure Port from [] to []** field until the appropriate port number or port range appears.

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

Toggle the **Speed/Duplex** field to select the speed and duplex/half-duplex state of the port. *Auto* means auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex mode. 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*.

Toggle the **Flow Control** field to disable or enable flow control for a specific port. 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.

Configure Bandwidth

The **Bandwidth Configuration** menu allows you to access screens that set and display the Ingress bandwidth and Egress bandwidth of specified ports on the Switch.

Highlight Configure Bandwidth on the Configuration menu and press Enter:

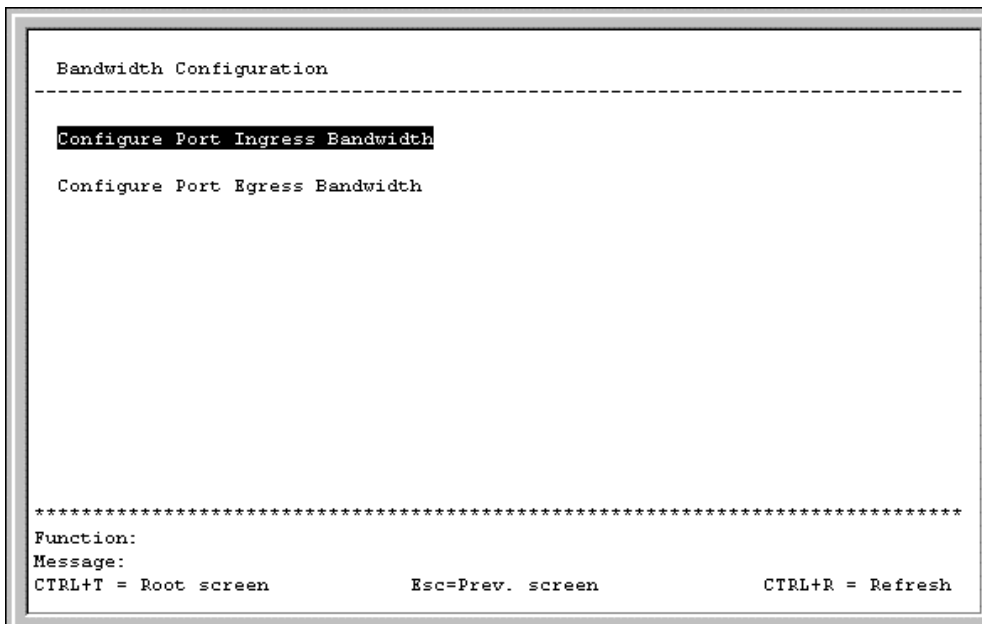


Figure 6-15. Bandwidth Configuration menu

To configure port ingress bandwidth, highlight **Configure Port Ingress Bandwidth** on the screen above and click **Enter**:

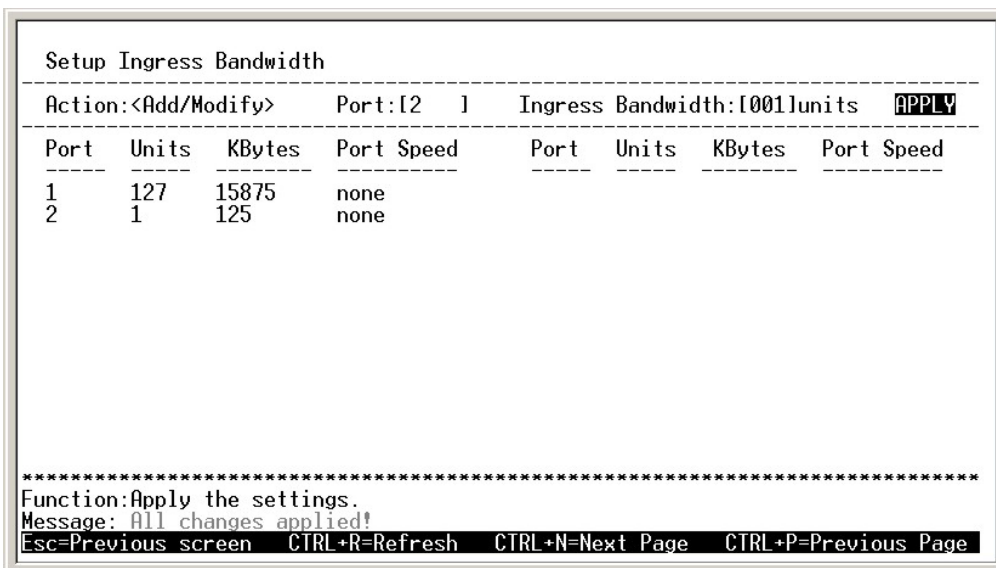


Figure 6-16. Setup Ingress Bandwidth screen

To configure ingress bandwidth for a specific port, adjust the following fields and press APPLY

Action: <Add/Modify> – Toggle to the desired option, *Add/Modify* or *Delete*.

Port: [1] – Choose which port you would like to configure the Ingress Bandwidth for.

Ingress Bandwidth [1] **units** – Setting this field for a particular port will allow the user to limit the amount of packets the switch can receive. For each port, an Ingress Bandwidth unit is valued at 125 Kbytes per second. The maximum value setting for this field is 127.

Included in this screen is a table showing the Ingress Bandwidth settings currently implemented on the switch. The *Port Speed* value displays the current speed setting of a certain port. If there is no connection or link to a port, *none* will be displayed.

To configure port egress bandwidth, highlight **Configure Port Egress Bandwidth** on the **Bandwidth Configuration** screen and click **Enter**:

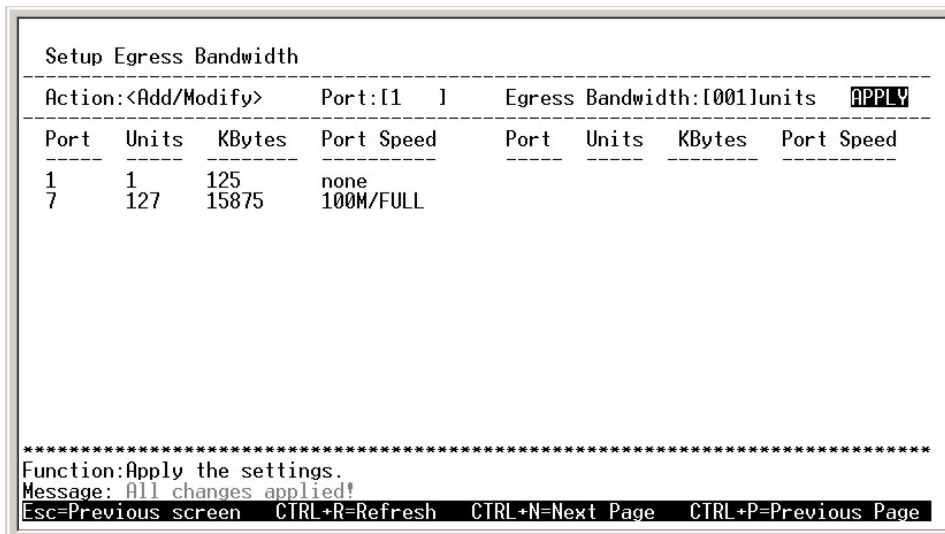


Figure 6-17. Setup Egress Bandwidth screen

To configure the egress bandwidth for a specific port, adjust the following fields and press APPLY

Action:<Add/Modify> – Toggle to the desired option, *Add/Modify* or *Delete*.

Port: [1] – Choose which port you would like to configure the Egress Bandwidth for.

Egress Bandwidth [1] units – Setting this field for a particular port will allow the user to limit the amount of packets the switch can send to a node. For each port, an Egress Bandwidth unit is valued at 125 Kbytes per second. The maximum value setting for this field is 127.

Included in this screen is a table showing the Egress Bandwidth settings currently implemented on the switch. The *Port Speed* value displays the current speed setting of a certain port. If there is no connection or link to a port, *none* will be displayed in the field.

Configure Spanning Tree Protocol

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

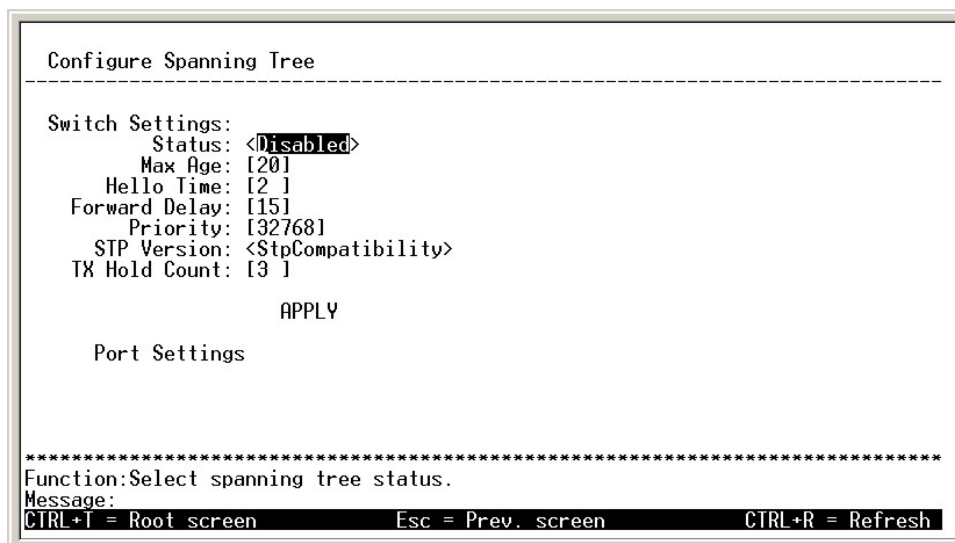


Figure 6-18. Configure Spanning Tree menu

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

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

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

Status: <Disabled> – Toggle to *Enabled* to implement the Spanning Tree Protocol on the Switch.

Max Age: [20] – The Maximum Age can be set from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Hello Time: [2] – The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

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

Forward Delay: [15] – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Priority: [32768] – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch.

STP Version: <StpCompatability> – Choose RSTP or STP Compatibility (default). 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.

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

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

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

Port Spanning Tree Settings

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

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

Port Spanning Tree Settings

View Ports: <1 to 12 > Configure Port from [1] to [1] STP Status: <Enabled >
 Cost: [0] Priority: [128] Migration: <No > Edge: <Yes > P-P: <Auto> APPLY

Port#	STP	Cost	Priority	Edge	P-P	Role	Port State
1	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
2	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
3	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
4	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
5	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
6	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
7	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
8	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
9	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
10	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
11	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled
12	Enabled	0/200000	128	Yes/Yes	Auto/Yes	-	Disabled

 Function: Select the scope of ports for display and configuration.
 Message:
 CTRL+I = Root screen Esc = Prev. screen CTRL+R = Refresh

Figure 6-19. Port Spanning Tree Settings screen

Toggle the **View Ports** field to the range of ports to be configured. The Fast Ethernet ports displayed for configuration in groups of 12 and the optional 100BASE ports are displayed together—if a 2-port rather than 1-port extension module is installed. Enter the port number or port range in the **Configure Port from [] to []** field. After enabling or disabling **STP Status**, you can set the spanning tree port cost and priority. Toggle the **Bypass** field to *Yes* if you want to enable the Switch to skip the usual waiting time associated with the listening state.

Configure Static (Destination-Address Filtering) Table

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

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

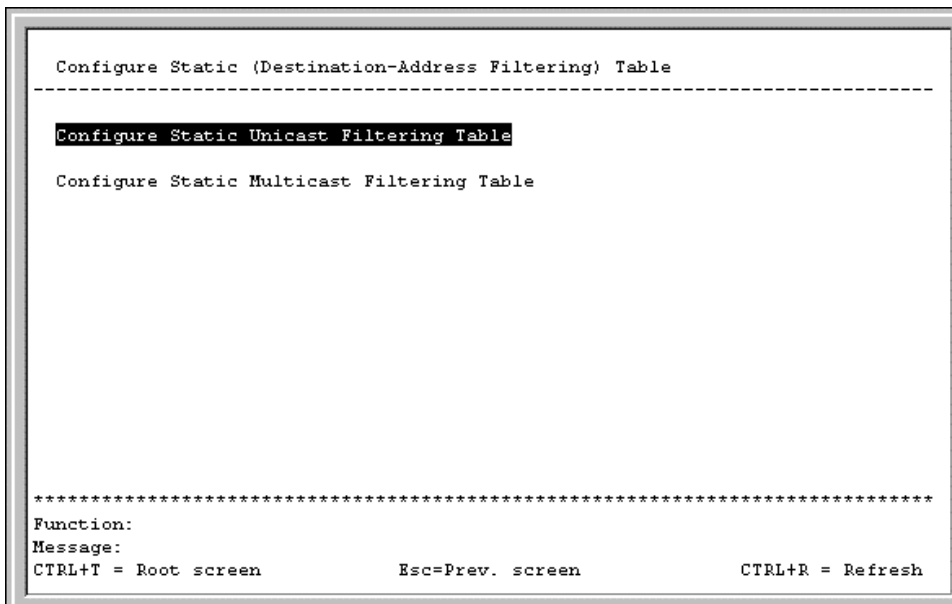


Figure 6-20. Configure Static (Destination-Address Filtering) Table menu

Setup Unicast Filtering Table

Highlight **Configure Static Unicast Filtering Table** on the menu to access the following screen:

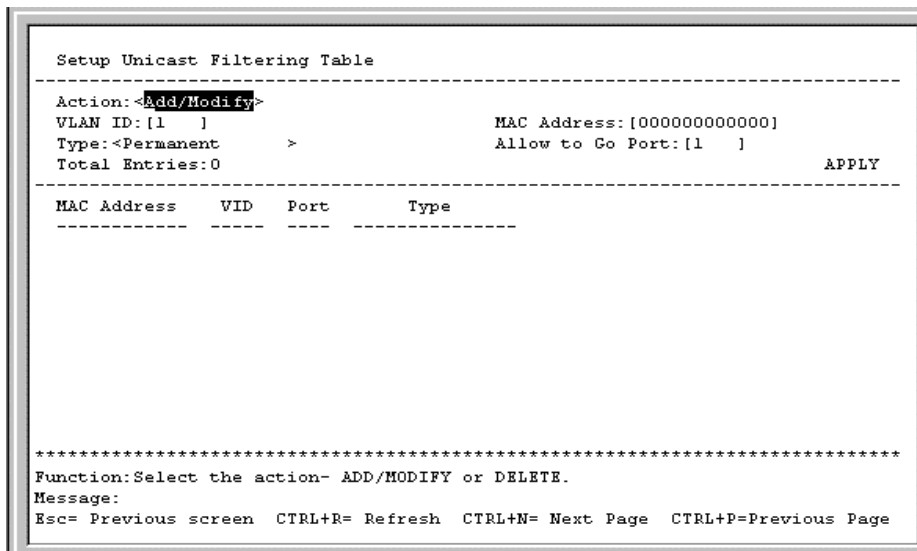


Figure 6-21. Setup Unicast Filtering Table screen

The **Action** field can be toggled between *Add/Modify* and *Delete* using the space bar. Enter the VID in the **VLAN ID** field and the MAC address to be statically entered in the forwarding table in the **MAC Address** field. There are two static unicast filter types to select from, *Permanent* and *DeleteOnReset*. Enter the port number in the **Allow to Go Port** field.

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

Setup Static Multicast Filtering Table

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

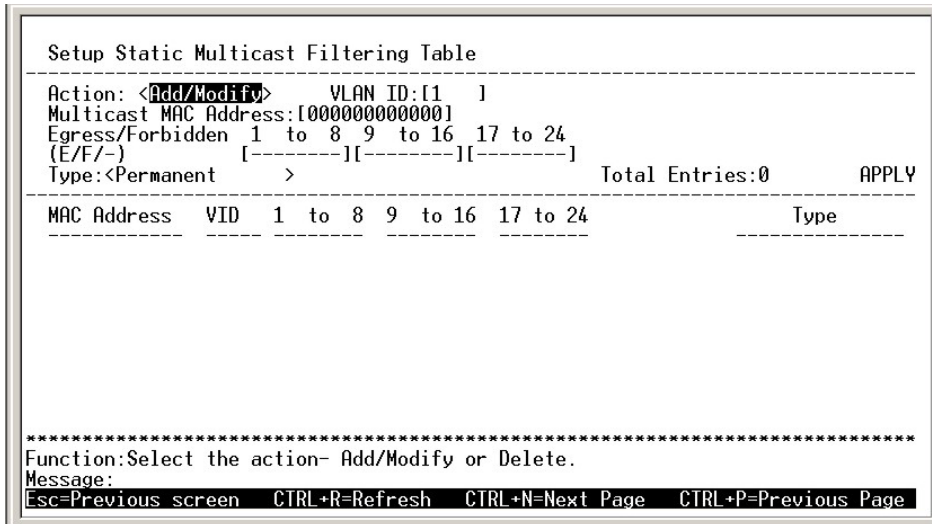


Figure 6-22. Setup Static Multicast Filtering Table screen

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

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

E (Egress Member) – Specifies the port as being a static member of the multicast group. Egress Member Ports are ports that will be transmitting traffic for the multicast group.

F (Forbidden Member) – Specifies the port as being forbidden from joining a VLAN dynamically.

- (Non-Member) – Specifies the port as not being a member of the multicast group, but the port can become a member of the multicast group dynamically.

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

Configure VLANs

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

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

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

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

To create a new 802.1Q VLAN:

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

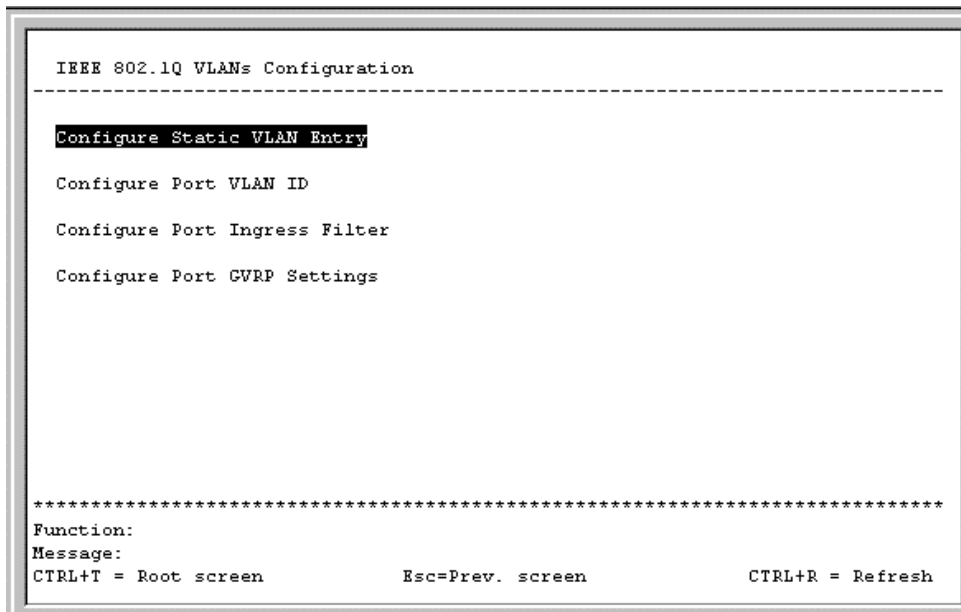


Figure 6-23. IEEE 802.1Q VLANs Configuration menu

802.1Q Static VLAN Settings

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

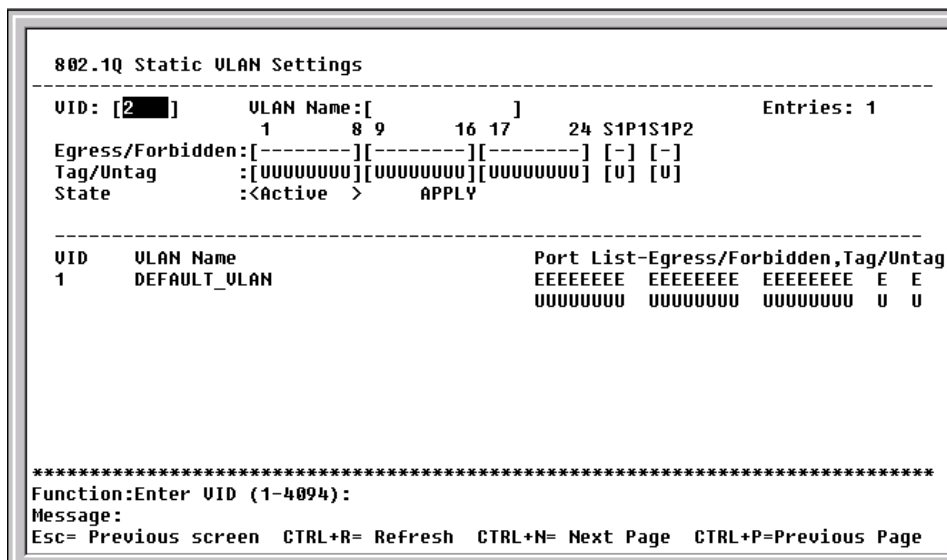


Figure 6-24. 802.1Q Static VLAN Settings screen

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

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

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

E (Egress Member) – Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.

F (Forbidden Non-Member) – Defines the port as a non-member and also forbids the port from joining a VLAN dynamically.

– (Non-Member) – Specifies the port as not being a member of the VLAN, but the port can become a member of the VLAN dynamically.

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

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

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

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

T - specifies the port as a Tagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the PVID (Port VLAN Identifier – see below). When a tagged packet exits the port, the packet header is unchanged.

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

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

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

Example of 802.1Q VLAN:

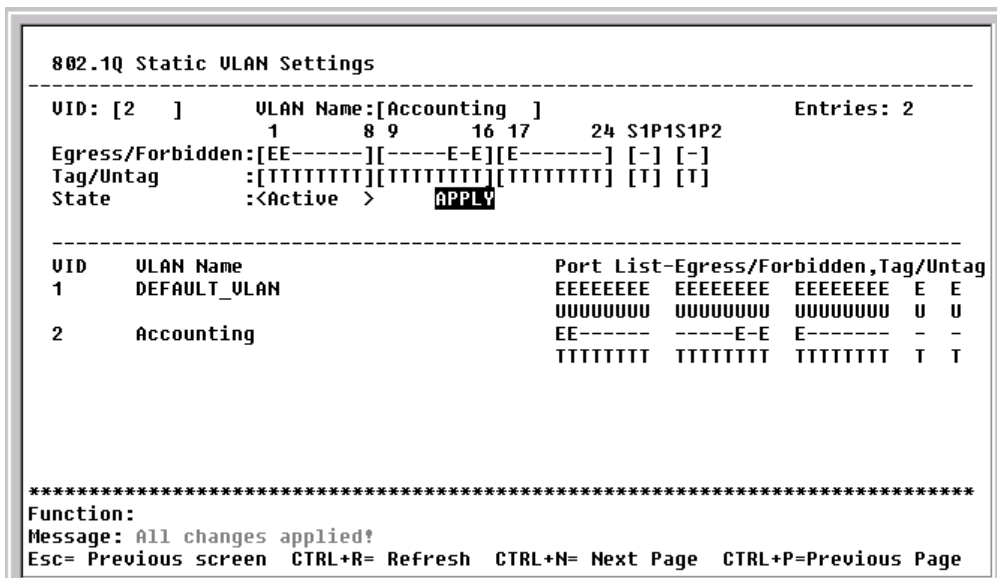


Figure 6-25. 802.1Q Static VLAN Settings screen

Port VLAN assignment

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

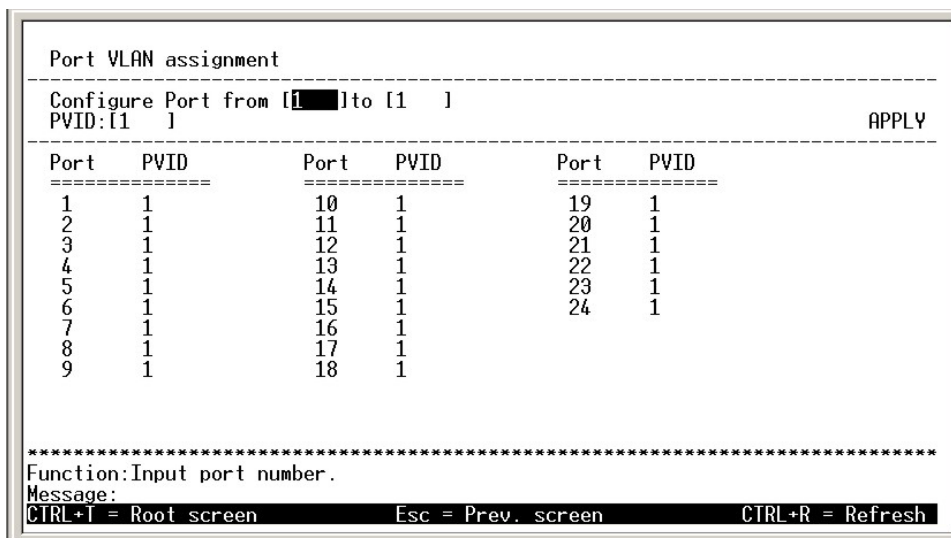


Figure 6-26. Port VLAN assignment screen

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

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

Ingress Filter Settings

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

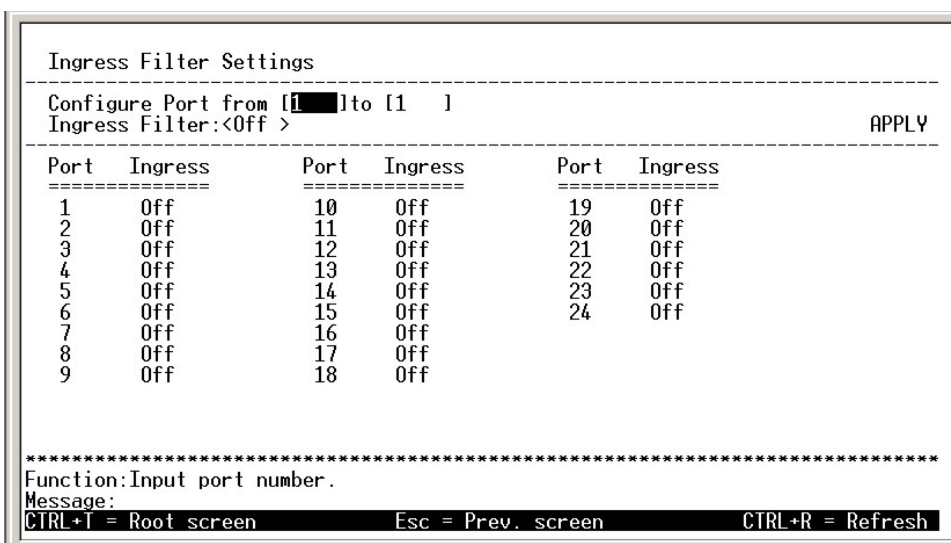


Figure 6-27. Ingress Filter Settings screen

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

An Ingress Filter enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet.

Port GVRP Settings

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

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

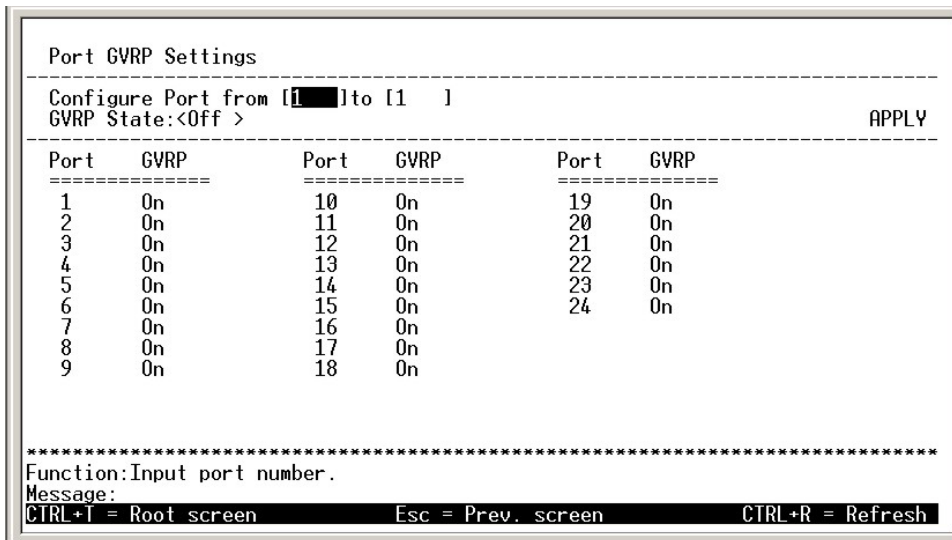


Figure 6-28. Port GVRP Settings screen

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

GVRP updates dynamic VLAN registration entries and communicates the new VLAN information across the network. This allows, among other things, for stations to physically move to other switch ports and keep their same VLAN settings, without having to reconfigure VLAN settings on the Switch.

Configure IGMP Snooping

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

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

```

IGMP Snooping Settings
-----
Switch IGMP Snooping: Disabled
*Notes: If you want to change it, back to Configure Switch.
Action: <Add/Modify>
VLAN ID:[1 ]          State:<Enabled >      Querier State:<Non-Querier>
Robustness Variable:[2 ] Query Interval:[125 ] Max Response:[10]  APPLY
-----
  VID   State   Age Out  Querier State
-----
  1     Enabled  260     Non-Querier

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

```

Figure 6-29. IGMP Snooping Settings screen

To configure IGMP Snooping:

Toggle the **Switch IGMP Snooping** field to *Enabled*. Toggle the **Querier State** field to the appropriate choice between *Non-Querier*, *V1-Querier*, and *V2-Querier* to determine the version of IGMP that is used in your network. A value between 1 and 255 can be entered for the **Robustness Variable** (default is 2). The **Query Interval** can be set between 1 and 65535 seconds (default is 125 seconds). This sets the time between IGMP queries. The **Max Response** allows a setting between 1 and 25 seconds (default is 10) and specifies the maximum amount of time allowed before sending a response report.

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

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

Switch IGMP Snooping:<Disabled> – This field can be toggled using the space bar between *Disabled* and *Enabled*. This is used to enable or disable IGMP Snooping, globally, on the Switch.

Action:<Add/Modify> – Toggle to the desired option, *Add/Modify* or *Delete*.

VLAN ID:[1] – Enter the appropriate VLAN ID in this field.

State:<Enabled> – Toggle this field to *Enabled* to activate this entry.

Querier State:<Non-Querier> – This field can be toggled between *Non-Querier*, *V1-Querier*, and *V2-Querier*. This is used to specify the IGMP version (1 or 2) that will be used by the IGMP interface when making queries.

Robustness Variable:[2] – A tuning variable to allow for sub-networks that are expected to lose a large number of packets. A value between 1 and 255 can be entered, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.

Query Interval:[125] – Allows the entry of a value between 1 and 65535 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.

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

Configure Port LACP Trunking

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

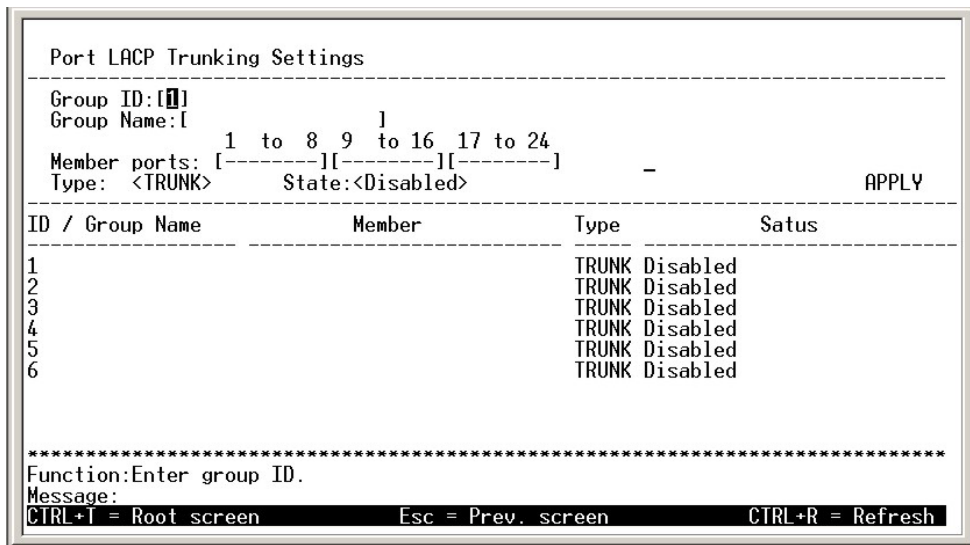


Figure 6-30. Port LACP Trunking Settings screen

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

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

The Switch allows the creation of up to 6 port trunking groups, each group consisting of up to 8 links (ports). The trunked ports can be non-continuous (that is, have non-sequential port numbers). All of the ports in the group must be members of the same VLAN. Further, the trunked ports must all be of the same speed and should be configured as full duplex.

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

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

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

The Link Aggregate Control Protocol (LACP) allows you to bundle several physical ports together to form one logical port. After the negotiation of LACP, these candidates of trunking ports could be trunked as a logical port. If any one of the connected ports pair has no LACP capability, these two ports will stand as regular ports until the success of LACP communication. Same as traditional port trunking as explained above, the member ports of a LACP trunk group only can be formed a trunk with a peer LACP trunk group.

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

Group ID:[I] – This field is for a group ID number for the port trunking group.

Group Name:[] – Enter a name for the port trunking group.

Member ports: [[] []] – Toggle between M to indicate membership of the port trunking group, or a dash (-) to indicate non-membership.

Type:<TRUNK> – Toggle between TRUNK and LACP. If LACP is selected, each member of the port trunking group must support the Link Aggregate Control Protocol. There is no protocol requirement if TRUNK is selected.

State:<Disabled> – This field can be toggled between Enabled and Disabled. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.

Configure Port Mirroring

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

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

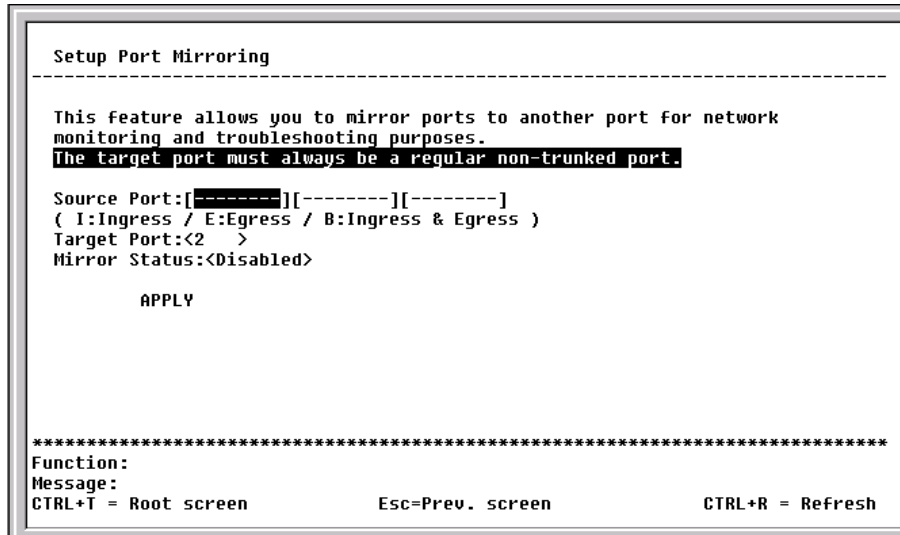


Figure 6-31. Setup Port Mirroring screen

To configure a mirror port, enter *I* (ingress), *E* (egress), or *B* (ingress & egress) for each port from where you want to copy frames in the **Source Port** field and then enter the port that receives the copies from the source port in the **Target Port** field. The target port is where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe. Finally, toggle the **Mirror Status** field to *Enabled*, highlight **APPLY**, and press **Enter**.

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

Configure Threshold of Broadcast/Multicast/DA-Unknown Storm

To configure the threshold of a broadcast, multicast, or DA (destination address)-Unknown Storm, select **Configure Threshold of Broadcast/Multicast/DA-Unknown Storm** on the **Configuration** menu and press **Enter**.

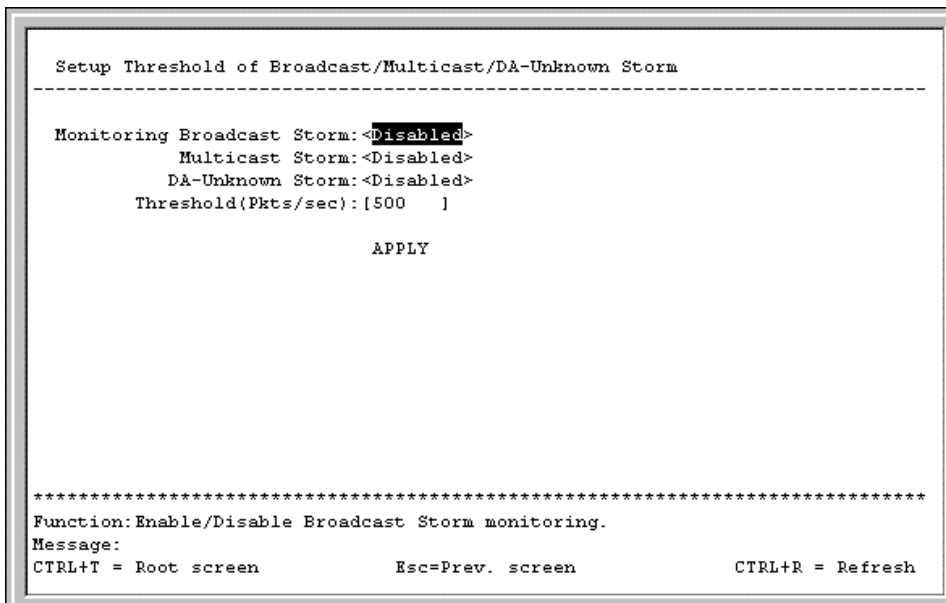


Figure 6-32. Setup Threshold of Broadcast/Multicast/DA-Unknown Storm screen

To use the features on this screen, toggle the desired option to *Enabled*, enter a threshold, and then press APPLY.

Configure Class of Service, Default Priority and Traffic Class

The DES-3210/DES-3218/DES-3226 allows you to customize class of service, port default priority, and traffic class settings on the following menu.

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

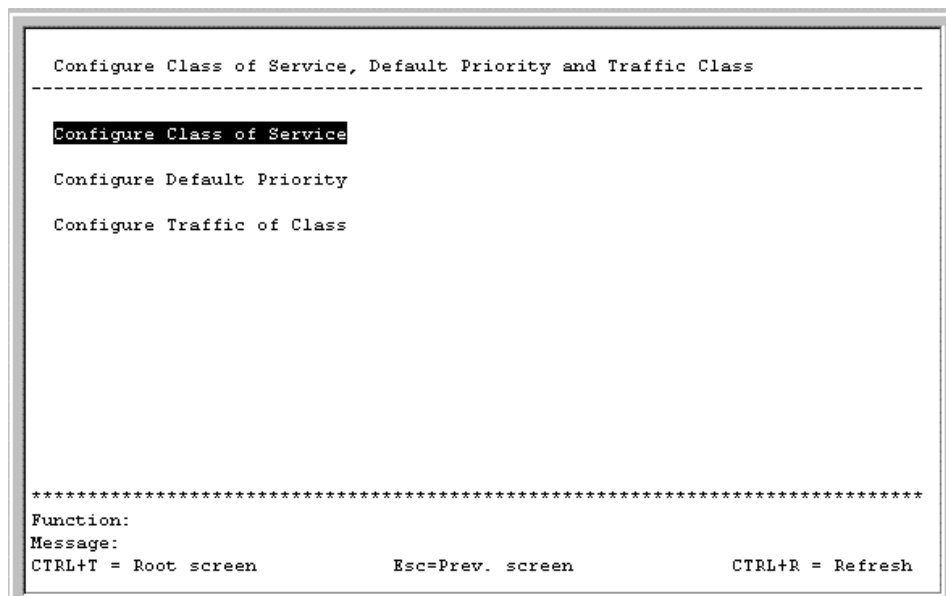


Figure 6-34. Configure Class of Service, Default Priority and Traffic Class menu

Class of Service Configuration

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

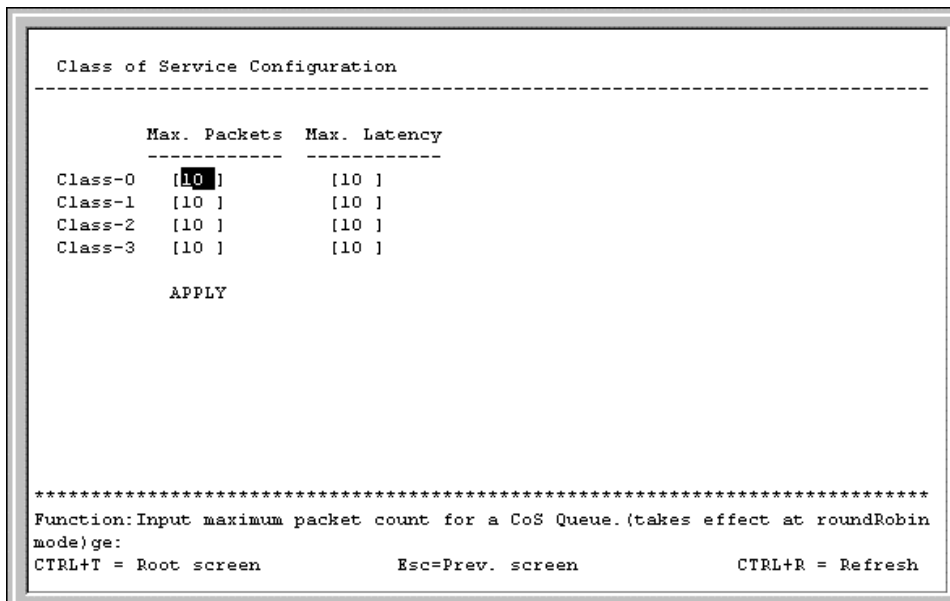


Figure 6-35. Class of Service Configuration screen

This screen allows you to set the following features:

Max. Packets – The Class of Service scheduling algorithm starts from the highest CoS for a given port, sends the maximum number of packets, then moves on to the next lower CoS. The values that can be entered in this field are from 1 to 255. Entering zero instructs the Switch to continue processing packets until there are no more packets in the CoS transaction queue.

Max. Latency – The maximum allowable time a packet will stay in the CoS queue. The packets in this queue are not delayed more than the maximum allowable latency entered in this field. The timer is disabled when this field is set to zero. Each unit of this timer is equal to 16 microseconds. Max. Latency takes precedence over the CoS scheduling algorithm.

Default Port Priority assignment

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

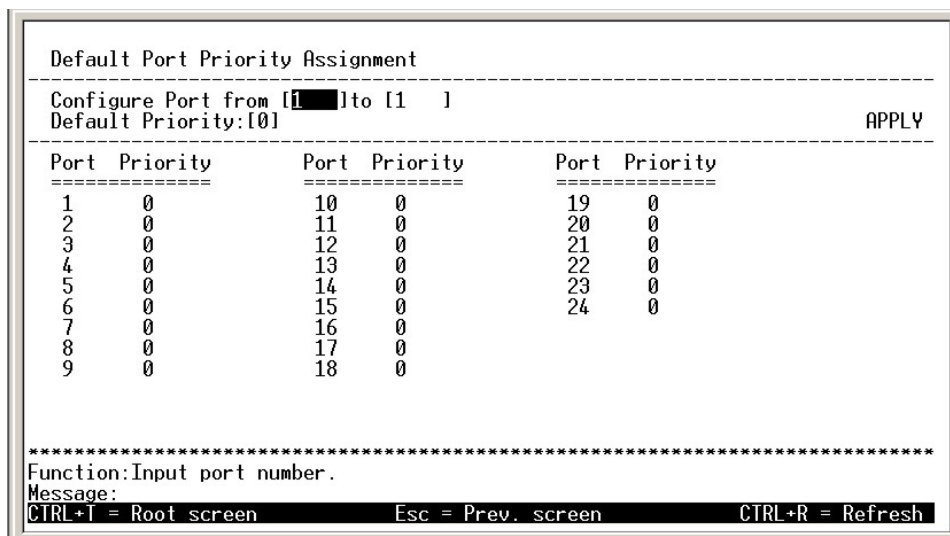


Figure 6-36. Default Port Priority Assignment screen

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

Class of Traffic Configuration

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

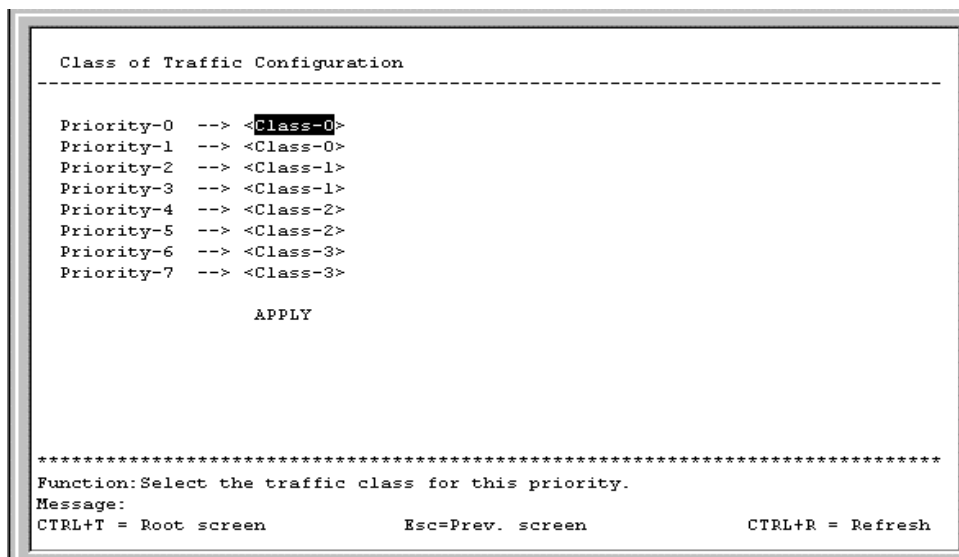


Figure 6-37. Class of Traffic Configuration screen

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

Configure Port GMRP Settings

Select **Configure Port GMRP Settings** and press **Enter** to access the following screen:

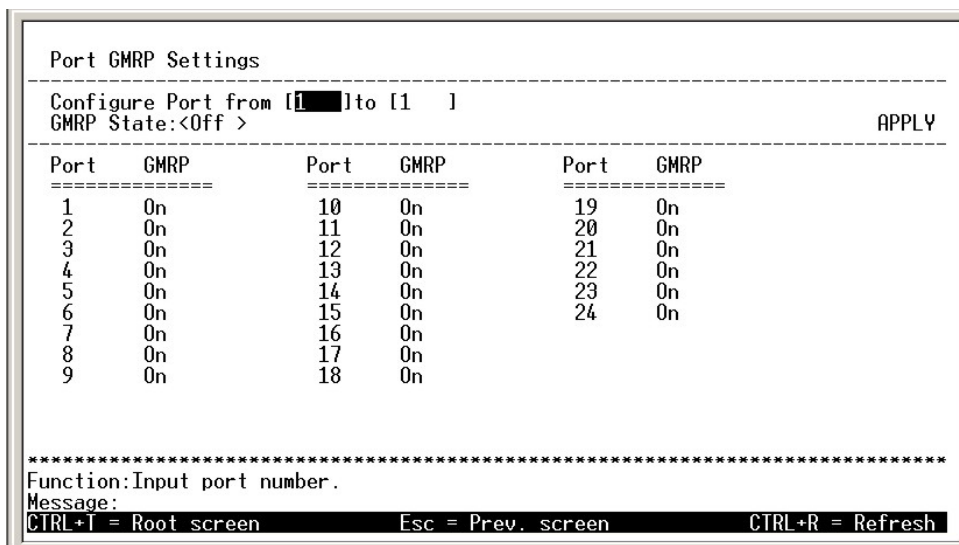


Figure 6-38. Port GMRP Settings screen

This screen allows you to enable Group Multicast Registration Protocol for individual ports by entering the port or port range in the first field, toggling **GMRP State** to *On* in the second field, and pressing **APPLY** to let your changes take effect.

Note: You must first enable GMRP globally on the **Configure Advanced Switch Features** screen before it can be used on the port level.

Configure DIFFSERV Settings

Select **Configure DIFFSERV Settings** and press **Enter** to access the following screen:

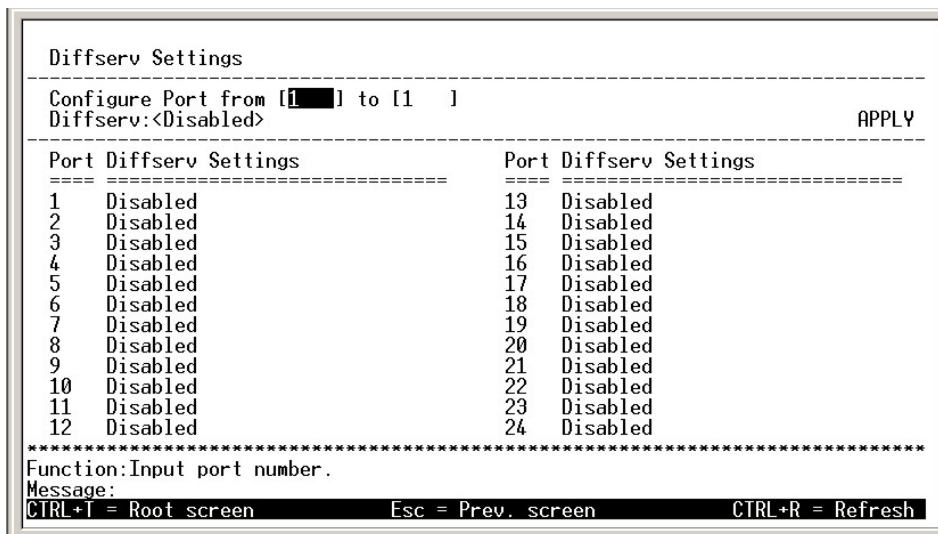


Figure 6-39. Diffserv Settings screen

Differentiated Services brings scalable Quality of Service to the Internet Protocol environment, using a Type of Service (TOS) field in the IP header. The Switch has the capability to change the TOS precedence field (the first 3 bits of the TOS field) based on the packet classification.

This screen allows you to set the following features:

Configure Port from [] to [] – Enter the port or ports to be set.

Diffserv – Choose from three options: *Disabled*, *DSCP*, and *TOS*.

Mode – Under *DSCP* (Differentiated Service Code Point), there are two choices, *Change if 0* or *Force Overwrite*. If *Force Overwrite* is selected, the differentiated services field of an incoming Ipv4 packet will be overwritten with the entered value. When *Change if 0* is selected, the differentiated services field of an incoming Ipv4 packet will be overwritten with the entered value if the original value of the DSCP field is zero. There are three choices under *TOS* (Type of Service): *TOS Overwrite 802.1p*, *802.1p Overwrite TOS*, and *Force Overwrite*. If *Force Overwrite* is selected, the IP TOS precedence of incoming Ipv4 packets will be overwritten with the entered value. If *TOS Overwrite 802.1p* is selected, the 802.1p tag control priority field of incoming Ipv4 packets will change to the value in the IP TOS precedence field. This action both alerts this field in the packet and changes the 802.1p priority used to determine the hardware CoS queue. If *802.1p Overwrite TOS* is selected, the IP TOS precedence of incoming Ipv4 packets will be changed to the value in the 802.1p tag control priority field.

DSCP value – Enter a DSCP value between 0 and 63 in this field.

TOS value – Enter a TOS value between 0 and 7 in this field.

Security Management

This section will help prepare the Switch user by describing the Port Security, Port Access Entity, Security IP, Security Shell and the Access Authentication Control all of which can be found under the Security Management Menu along with various submenus.

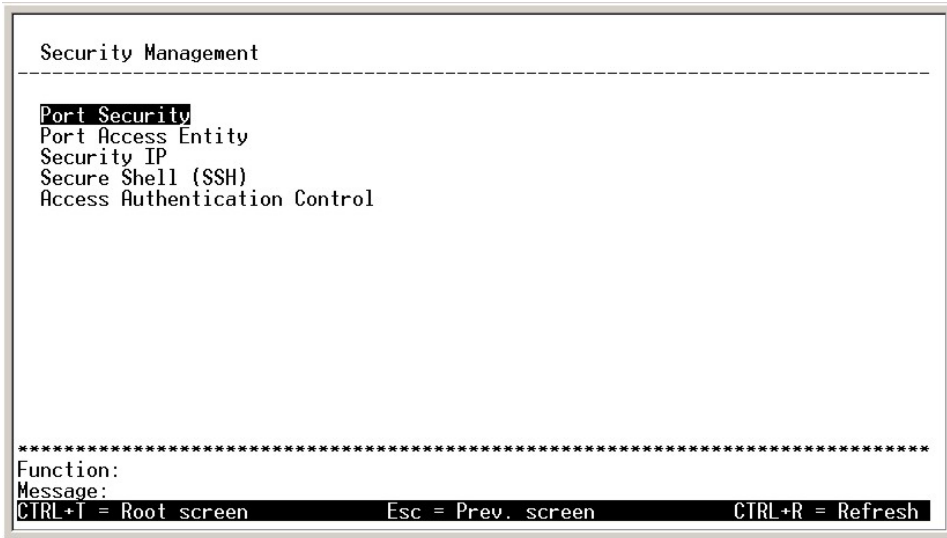


Figure 6- 40. Security Management menu

Configure Port Security

To configure security for a specified port or range of ports on the Switch, select **Port Security** on the **Security Management** menu and press **Enter**.

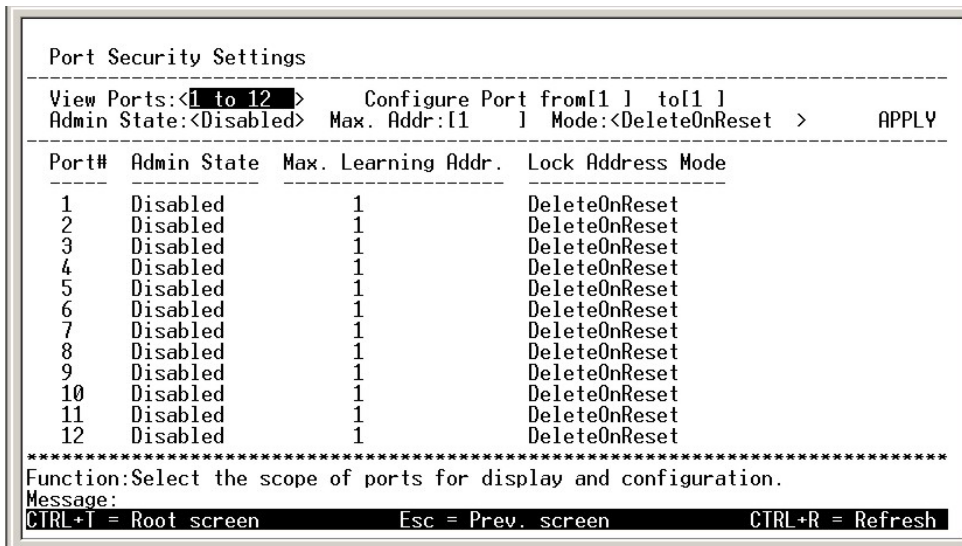


Figure 6-41. Port Security Settings screen

To set up security for a port or ports, toggle **View Ports** to the desired range, enter the port or ports in the next field, toggle **Admin State** to *Enabled*, enter the maximum number of addresses, the desired **Mode**, and then press **APPLY**.

Configure Port Access Entity

The DES-3210/DES-3218/DES-3226 allows you to set the authentication status of individual ports on your Switch on the following menu.

Select **Port Access Entity** on the **Security Management** menu and press **Enter**.

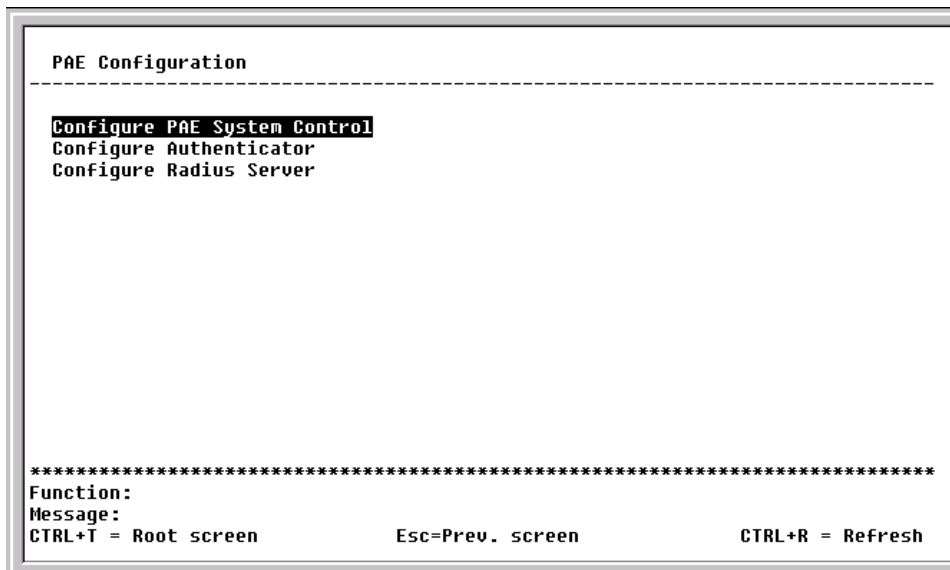


Figure 6-42. PAE Configuration menu

PAE System Configuration

Select **Configure PAE System Control** and press **Enter** to access the following menu:

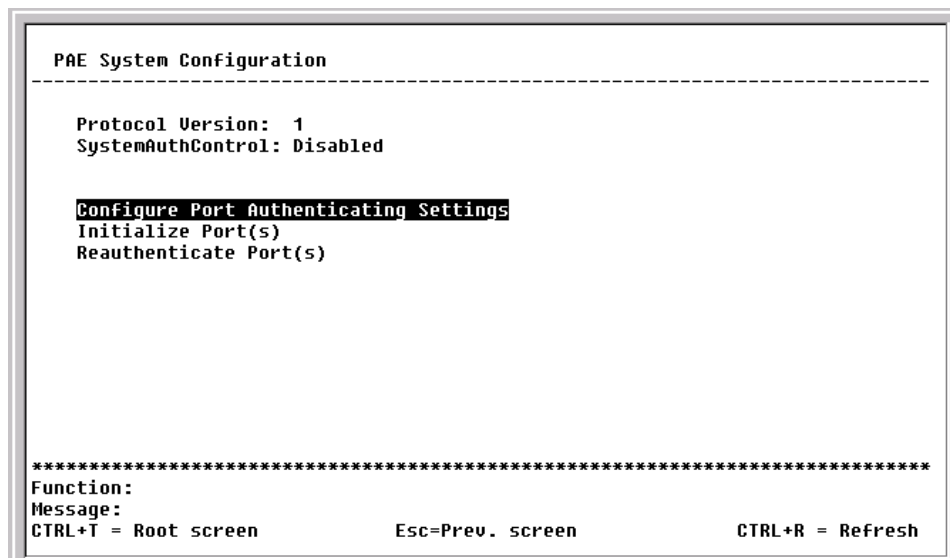


Figure 6-43. PAE System Configuration menu

This menu displays the current Protocol Version being used and the status of the SystemAuthControl. It also allows you to access the following three additional Port Access Entity System Configuration screens.

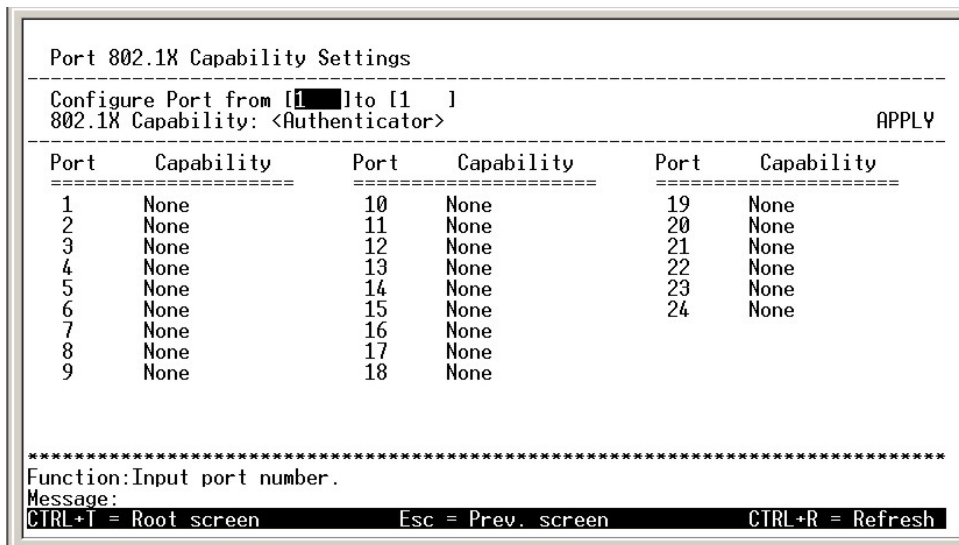


Figure 6-44. Port 802.1X Capability Settings screen

To set up the Switch's 802.1X port-based authentication, select which ports are to be configured in the **Configure Port from [] to []** field. Next, enable the selected ports by toggling the **802.1X Capability** field to *Authenticator*. Press APPLY to let your change take effect.

Note: You cannot configure a port to *Authenticator* when it is either a trunk port or LACP member port.

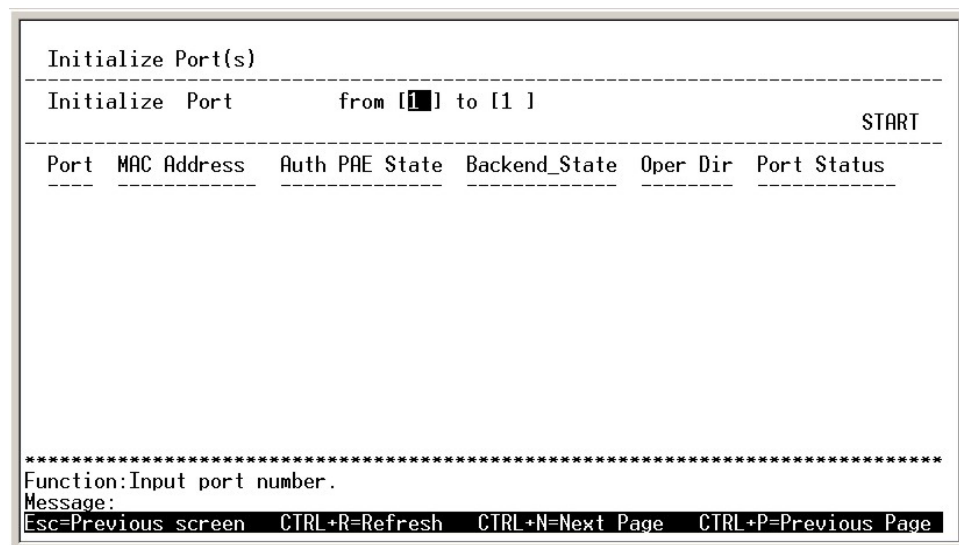


Figure 6-45. Initialize Port(s) screen

This screen allows you to initialize a port or group of ports. The table also displays the current status of the port(s) once you press START.

This screen displays the following information:

Port – The port number.

MAC Address – Displays the physical address of the switch where the port resides.

AuthState – The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.*

BackendState – The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.*

OprDir – The Operational Controlled Directions are *both* and *in*.

PortStatus – The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

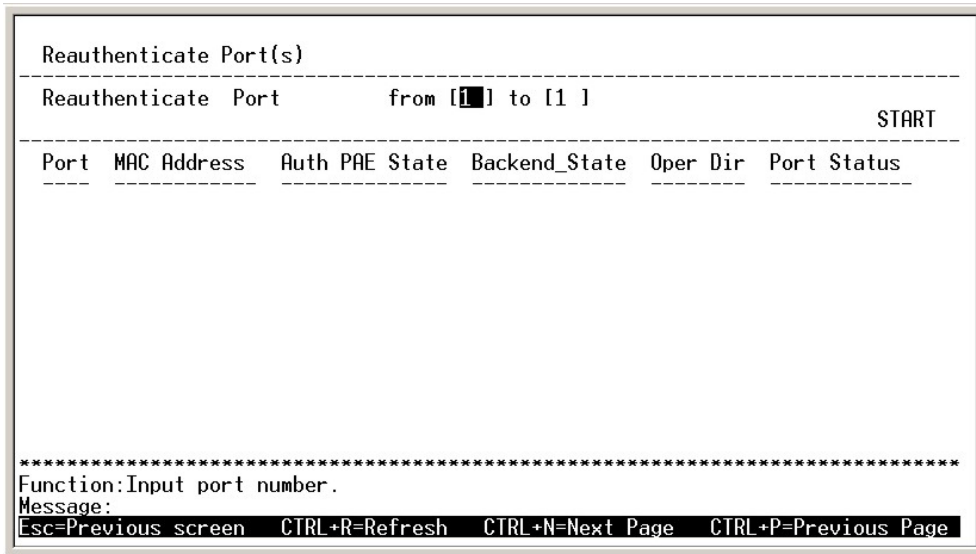


Figure 6-46. Reauthenticate Ports(s) menu

This screen allows you to reauthenticate a port or group of ports. The table also displays the current status of the port(s) once you press START.

This screen displays the following information:

Port – The port number.

MAC Address – Displays the physical address of the switch where the port resides.

Auth PAE State – The Authenticator PAE State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, *ForceUnauth*, and *N/A*.

BackendState – The Backend Authentication State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize*, and *N/A*.

OprDir – The Operational Controlled Directions are *both* and *in*.

PortStatus – The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

Configure 802.1X – Authenticator Configuration

Select **Configure Authenticator** on the **PAE Configuration** menu and press **Enter** to access the following screen:

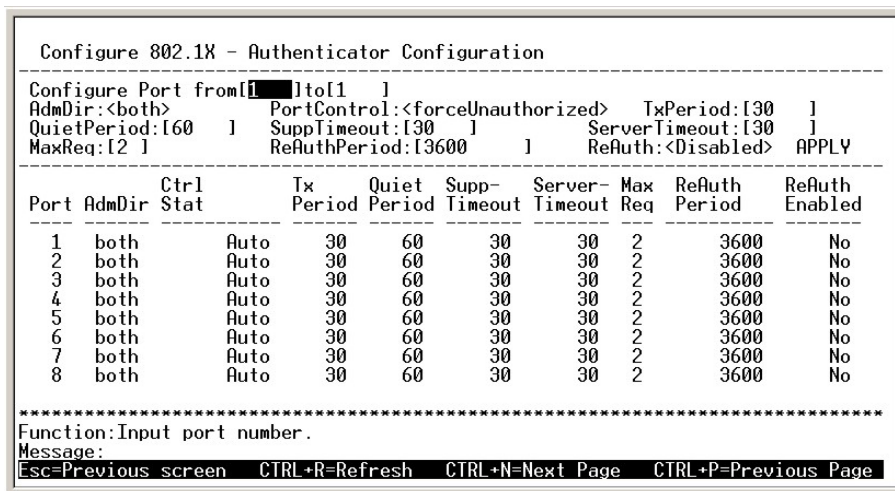


Figure 6-47. Configure 802.1X – Authenticator Configuration screen

This screen allows you to set the following features:

Configure Port from [] to [] – Enter the port or ports to be set.

AdmDir:<both> – Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

PortControl:<auto> – This allows you to control the port authorization state. Select *forceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *forceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. The third option is *auto*. This enables 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

TxPeriod:[30] – This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client.

QuietPeriod:[60] – This allows you to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.

SuppTimeout:[30] – This value determines timeout conditions in the exchanges between the Authenticator and the client.

ServerTimeout:[30] – This value determines timeout conditions in the exchanges between the Authenticator and the authentication server.

MaxReq:[2] – The maximum number of times that the switch will retransmit an EAP Request to the client before it times out of the authentication sessions

ReAuthPeriod:[3600] – A constant that defines a nonzero number of seconds between periodic reauthentication of the client.

ReAuth:<Disabled> – Determines whether regular reauthentication will take place on this port.

Configure Radius Server

Select **Configure Radius Server** on the **PAE Configuration** menu and press **Enter** to access the following screen:

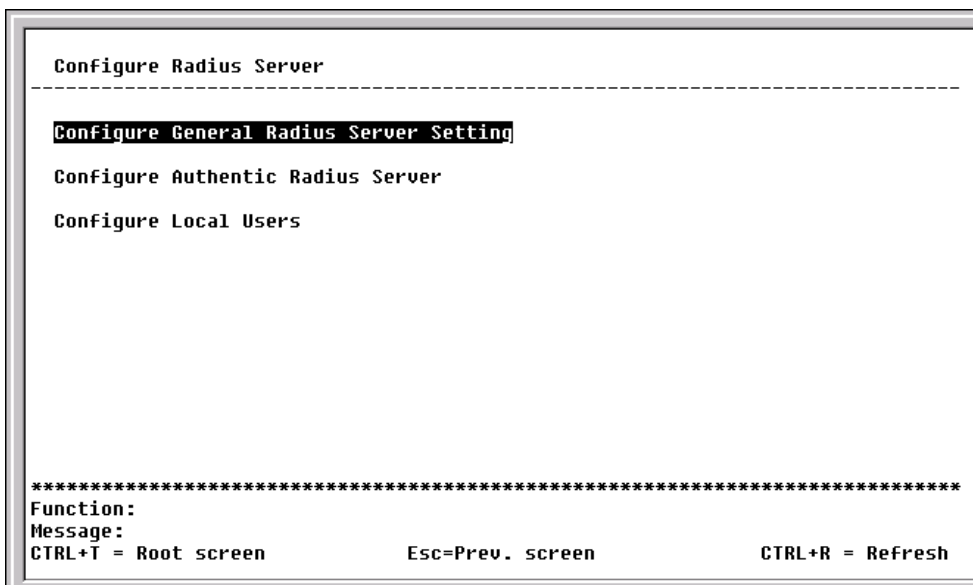


Figure 6-48. Configure Radius Server menu

This menu offers four configuration choices for the radius server.

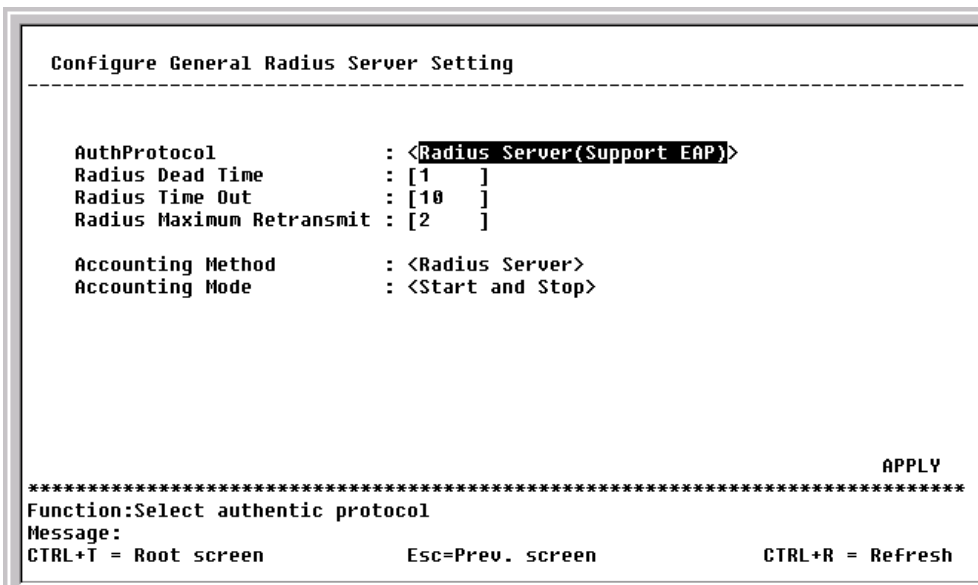


Figure 6-49. Configure General Radius Server Setting screen

This screen allows you to set the following features:

AuthProtocol: <Radius Server(Support EAP)> – Toggle between the authentication protocol options: *Radius Server(Support EAP)* and *Local*. In *Local* mode, use local authenticating (based on local user settings) rather than a remote RADIUS server.

Radius Dead Time:[1] –This specifies the number of minutes a RADIUS server which is not responding to authentication requests is considered unavailable and is passed over by further requests for RADIUS authentication.

Radius Time Out:[10] – This specifies the number of seconds NAS waits for a reply to a RADIUS request before transmitting the request.

Radius Maximum Retransmit:[2] –This specifies the number of times NAS transmits each RADIUS request to the server before giving up.

Accounting Method:<Radius Server> – To use a RADIUS Server, toggle from *None* to *Radius Server*.

Accounting Mode:<Start and Stop> – Select the desired method: *Start and Stop*, *Stop only*, or *None*.

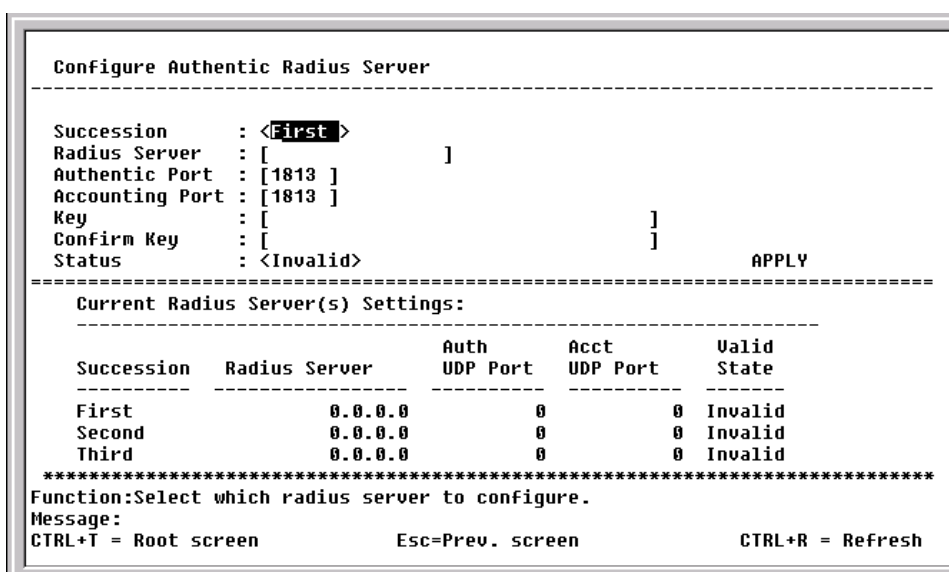


Figure 6-50. Configure Authentic Radius Server screen

This screen allows you to set the following features:

Succession: <First> – Choose the desired RADIUS server to configure: *First*, *Second* or *Third*.

Radius Server: [0.0.0.0] – Set the RADIUS server IP.

Authentic Port: [1813] – Set the RADIUS authentic server(s) UDP port. The default value is 1813.

Accounting Port: [1813] – Set the RADIUS account server(s) UDP port. The default value is 1813.

Key – Set the key the same as that of the RADIUS server.

Confirm Key – Confirm the shared key is the same as that of the RADIUS server.

Status:<Invalid> –This allows you to set the RADIUS server as *Valid* or *Invalid*.

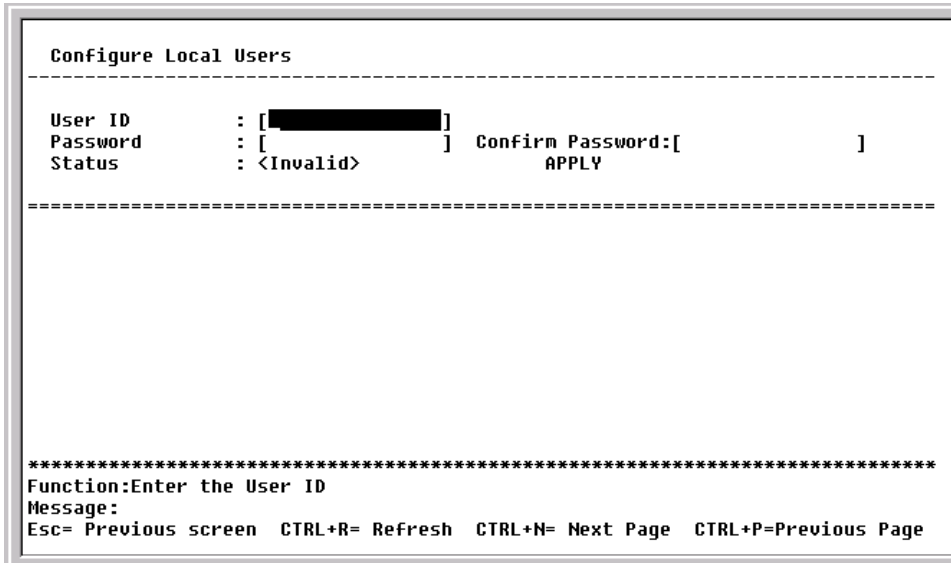


Figure 6-51. Configure Local Users screen

The fields on this screen allow you to add or remove local users.

Security IP

To configure a list of IP addresses that can access the switch, select **Security IP** on the **Security Management** menu and press Enter.

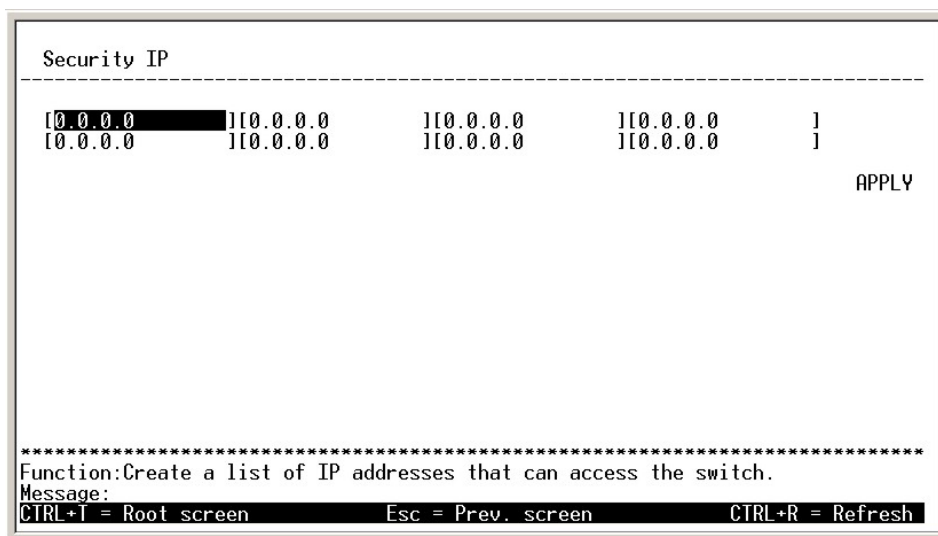


Figure 6- 52. Security IP screen

Enter the IP address(es) into the spaces provided, highlight **APPLY** and press **Enter**.

Note: Your local host IP address must be one of the IP addresses to avoid disconnection.

Secure Shell

Secure Shell (SSH) is a mechanism for allowing secure remote access to management functions on a device. SSH provides a function similar to Telnet. Users can log into and configure the device using a publicly or commercially available SSH client program, just as they can with Telnet. However, unlike Telnet, which provides no security, SSH provides a secure, encrypted connection to the device.

SSH supports Arcfour, AES, IDEA, Blowfish, DES (56-bit) and 3DES (168-bit) data encryption methods. Ten levels of data compression are available. You can configure your SSH client to use any one of these data compression levels when connecting to a device.

To access the Secure Shell menu, highlight Secure Shell (SSH) on the Security Management menu and press Enter.

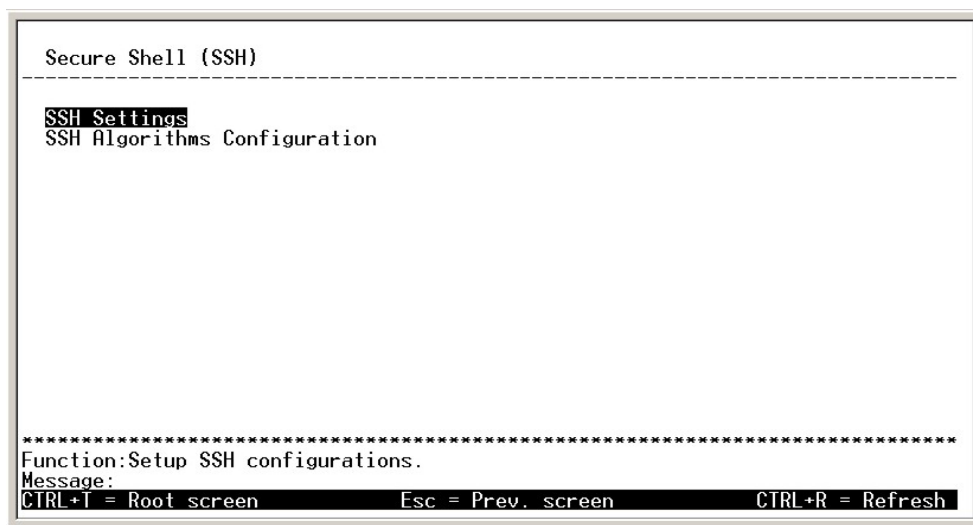


Figure 6- 52. Secure Shell menu

SSH Settings

To access the settings for the Secure Shell, highlight **SSH Settings** on the **Secure Shell** menu and press **Enter**.

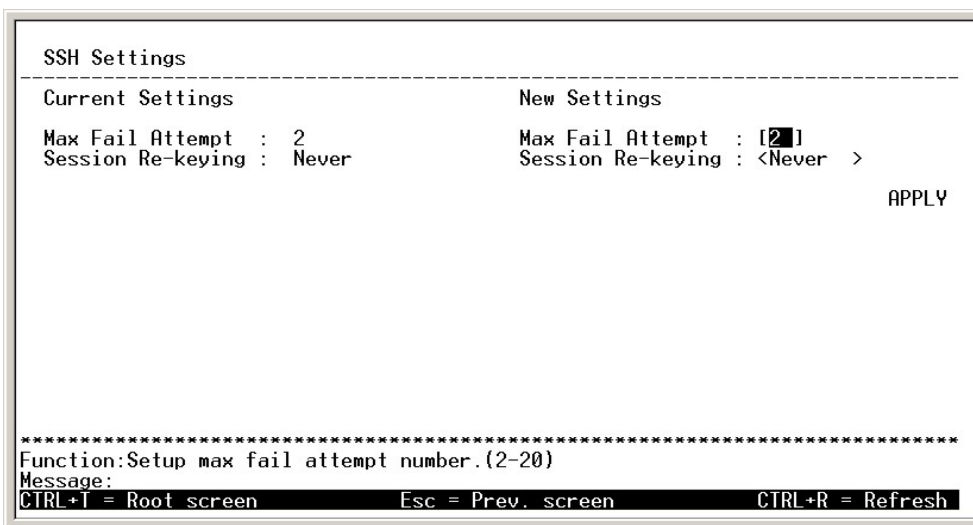


Figure 6- 53. SSH Settings screen

This screen shows the current **Secure Shell** settings and allows the user to alter them, under the *New Settings* header. The user may adjust:

Max Fail Attempt: [2] – Attempts may be set from 2 to 20 (default=2). Allows the user to set the number of times an outside guest may attempt to log on to the switch. With the **Max Fail Attempt** set at the default setting of 2, the outside guest must enter the appropriate settings within two attempts or that guest will have to start a new session.

Session Re-keying: [Never] – Sets the time period that the switch will change the security shell encryptions. Settings may be toggled to *Never*, *10 min*, *30 min*, and *60 min*.

SSH Algorithms Configuration

To configure the SSH Algorithms, highlight **SSH Algorithms Configurations** on the **Secure Shell** menu and press **Enter**.

```

SSH Algorithms Configuration
-----
Encryption Algorithm                Data Integrity Algorithm
3DES-cbc      : <Enabled >
Blow-fish-cbc : <Enabled >
AES128-cbc    : <Enabled >
AES192-cbc    : <Enabled >
AES256-cbc    : <Enabled >
Arcfour       : <Enabled >
Cast128-cbc   : <Enabled >
Twofish128    : <Enabled >
Twofish192    : <Enabled >
Twofish256    : <Enabled >

                                HMAC-SHA1      : <Enabled >
                                HMAC-MD5       : <Enabled >

                                Key Exchange Algorithm
                                Diffie-Hellman : <Enabled >

                                Authentication Algorithm
                                Password        : <Enabled >
                                Publickey      : <Enabled >
                                Host-based     : <Enabled >

                                APPLY
*****
Function: Setup 3DES encryption algorithm.
Message:
CTRL+I = Root screen      Esc = Prev. screen      CTRL+R = Refresh

```

Figure 6- 54. SSH Algorithms Configuration screen

Encryption Algorithm: Allows the user to *Enable* or *Disable* encryption algorithms set in the device. When a client connects, it will select which algorithms to use from the list of algorithms specified by the user.

Data Integrity Algorithm: Choose the Data Integrity algorithm to apply to traffic on the switch. Your selection of an Data Integrity algorithm determines how IP packets are exchanged between the client and the server. The user may *Enable* or *Disable* HMAC-SHA1 (hashing message authentication codes using the SHA cryptographic) and HMAC-MD5 (message digest algorithm hashing function).

Key Exchange Algorithm: This algorithm allows two users to exchange a secret key over an insecure medium without any prior secrets. The user may *Enable* or *Disable* this algorithm.

Authentication Algorithm: These settings allow the user to choose the algorithms the client can access the switch with. The user may *Enable* or *Disable* Password, Publickey or Host-based encryptions.

Access Authentication Control

The Access Authentication Control feature provides a way to centrally validate users attempting to gain access to the switch using the Terminal Access Controller Access Control System (TACACS) protocol. TACACS is implemented in the switch's software to allow centralized control over access to servers. Authentication can also be provided for administrative tasks on the server and access server user interfaces. With TACACS enabled, the access server prompts the user accessing the switch for a username and password, and then verifies the password with TACACS.

There are currently three versions of the TACACS security protocol, each a separate entity. The switch's software supports the following versions of TACACS:

- TACACS+—Provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through Authentication, Authorization, and Accounting (AAA) and can be enabled only through AAA commands.

- Extended TACACS (XTACACS)—Provides information about protocol translator and router use. This information is used in UNIX auditing trails and accounting files.
- TACACS—Provides password checking and authentication, and notification of user actions for security and accounting purposes

Note: Authentication, Authorization, and Accounting (AAA) network security services provide the primary framework through which you set up access control on your router or access server.

Under the **Security Management** menu, highlight **Access Authentication Control** and press enter.

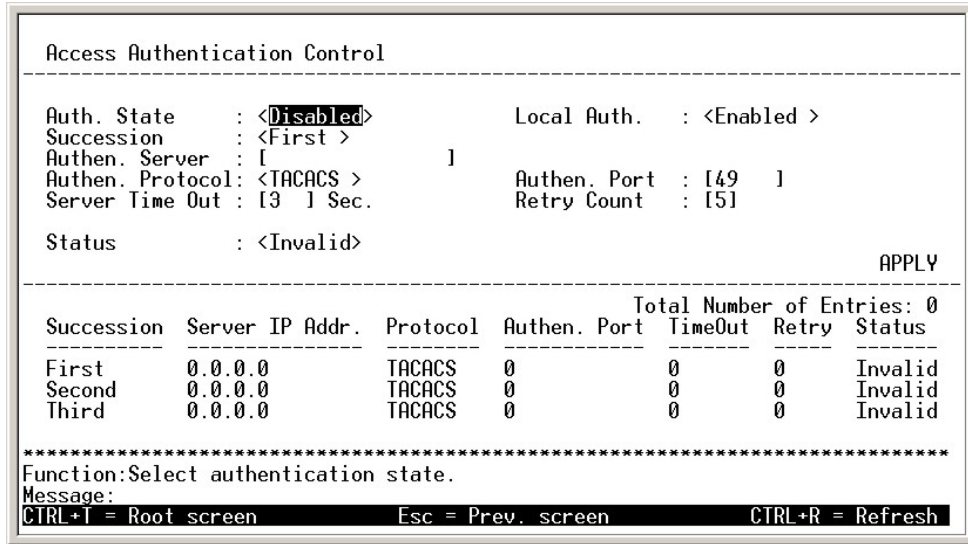


Figure 6- 55. Access Authentication Control screen

To configure the Access Authentication Control for an IP address, the following fields must be set:

Auth. State: (Authentication State)<Disabled> – Toggled the field to *Enabled* to implement the TACACS protocol. If the **Auth. State** is *Enabled*, the **Local Auth.** must be *Disabled*.

Local Auth: Enabled> – This field must be toggled to *Disabled* for the TACACS protocol to be implemented. If Enabled, the switch will use the local authentication already implemented.

Succession: <First> – A total of three servers are supported for TACACS/TACACS+ authentication. Toggle between First, Second and Third to determine the order required by the user.

Authen. Server: [] – Enter the IP address of the server to be authenticated.

Authen. Protocol: <TACACS> – Toggle between TACACS, TACACS+ and XTACACS, depending on the security protocol desired. A brief description of each is listed above. Using TACACS+, two new fields will appear:

Key: [] – Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

Confirm Key: [] – Retype the same key to verify.

Authen. Port: [49] – Edit the number in this field to change the port number from the default value of 49.

Server Time Out: [3] – Edit the value in the Server Time Out field to change how many seconds the device waits for a response from the TACACS server before either retrying the authentication request or determining that the TACACS server is unavailable and moving on to the next authentication method in the authentication-method list. The default is 3 seconds.

Retry Count: [5] – Edit the value in the Retry Count field to change how many times the device will resend an authentication request when the TACACS server does not respond.

Status: <Invalid> – Toggle to *Valid* to implement the server IP address with TACACS security enabled.

Highlight APPLY and press Enter to implement the settings.

Network Monitoring

The DES-3210/DES-3218/DES-3226 provides extensive network monitoring capabilities.

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

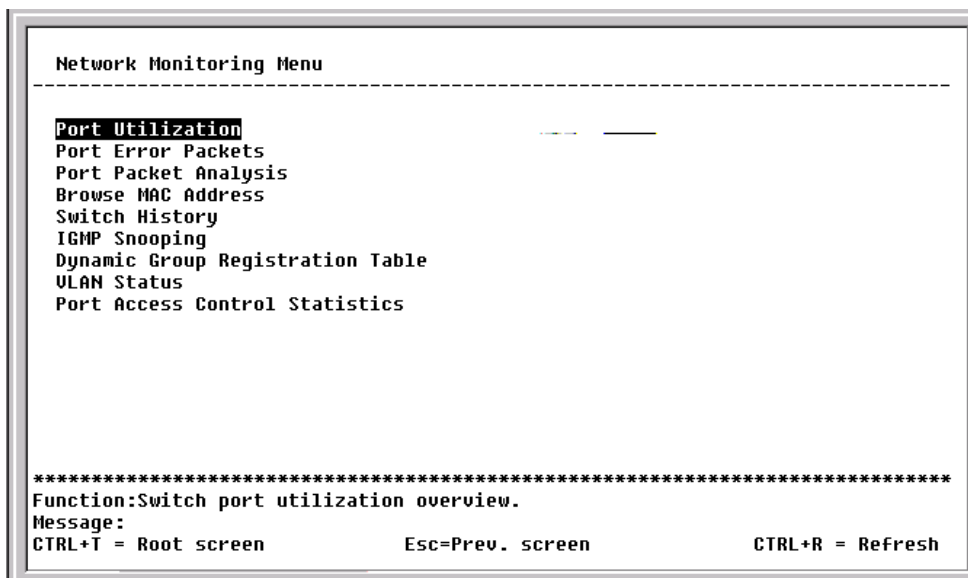


Figure 6-56. Network Monitoring Menu

Port Utilization

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

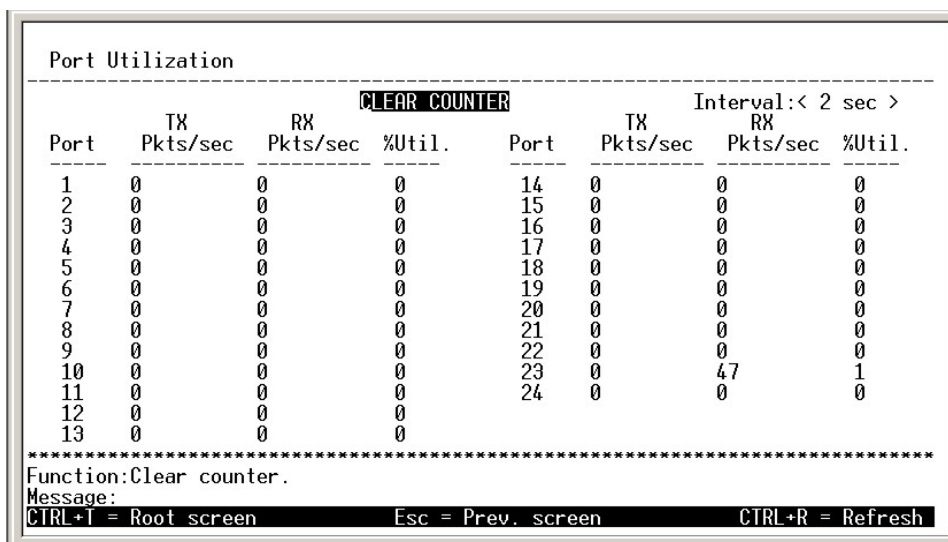


Figure 6-57. Port Utilization screen

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

Port Error Packets

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

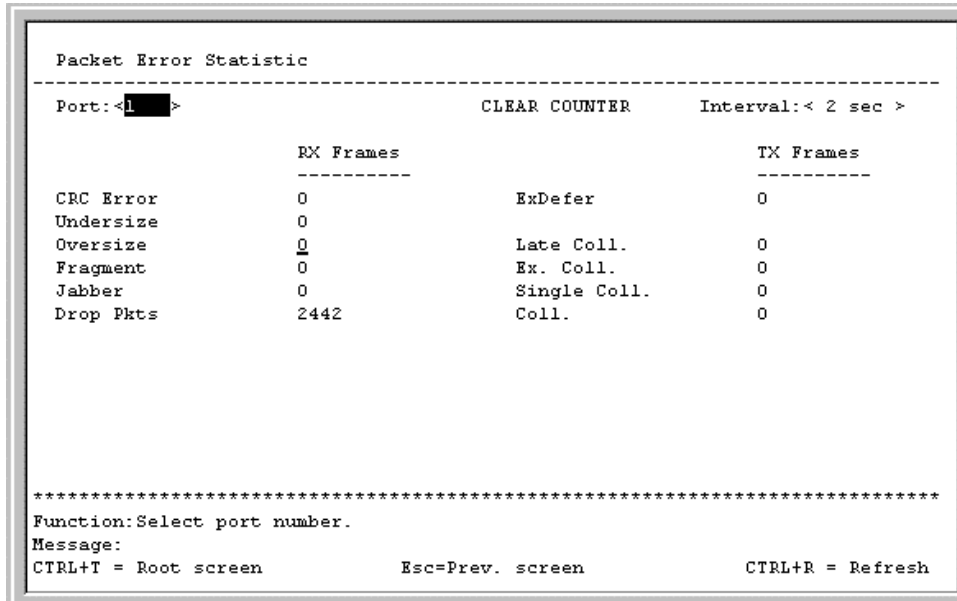


Figure 6-58. Port Error Statistic screen

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

Port Packet Analysis

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

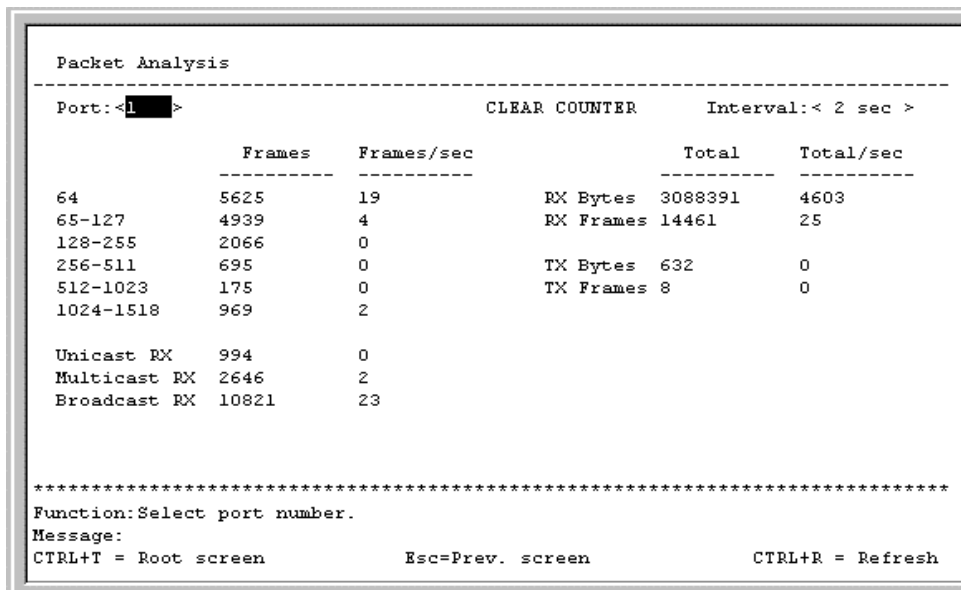


Figure 6-59. Packet Analysis table

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

Browse MAC Address

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

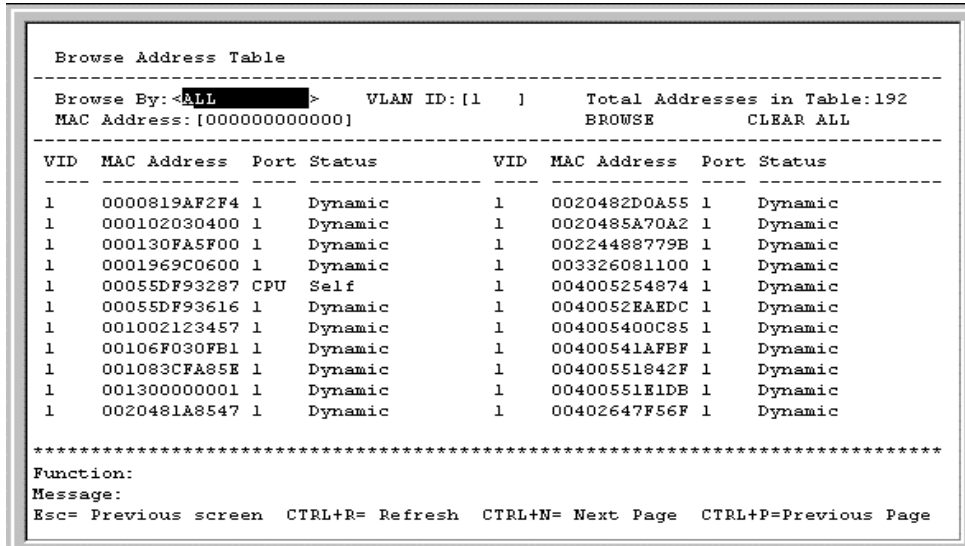


Figure 6-60. Browse Address Table screen

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

To search for a particular MAC address:

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

Switch History

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

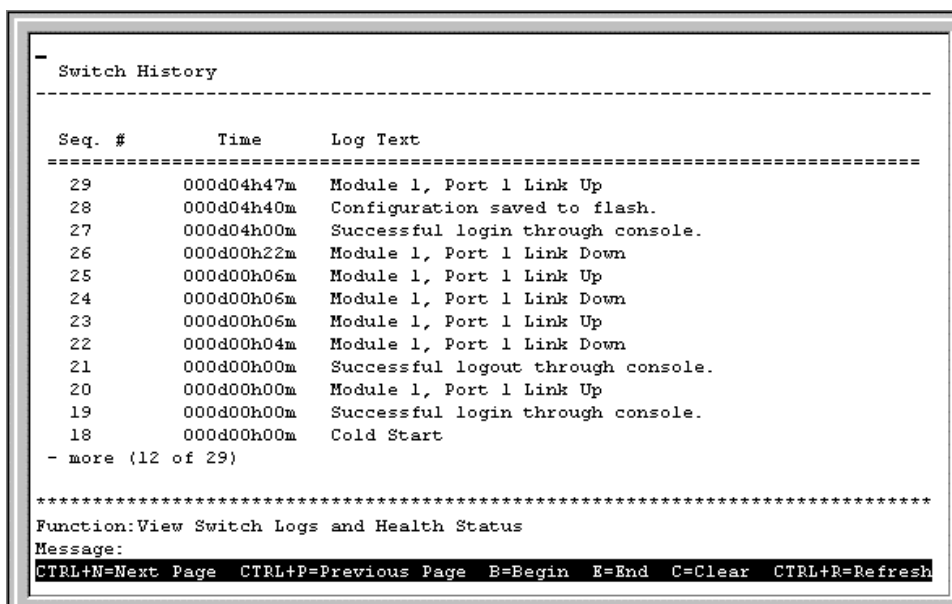


Figure 6-61. Switch History screen

IGMP Snooping

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

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

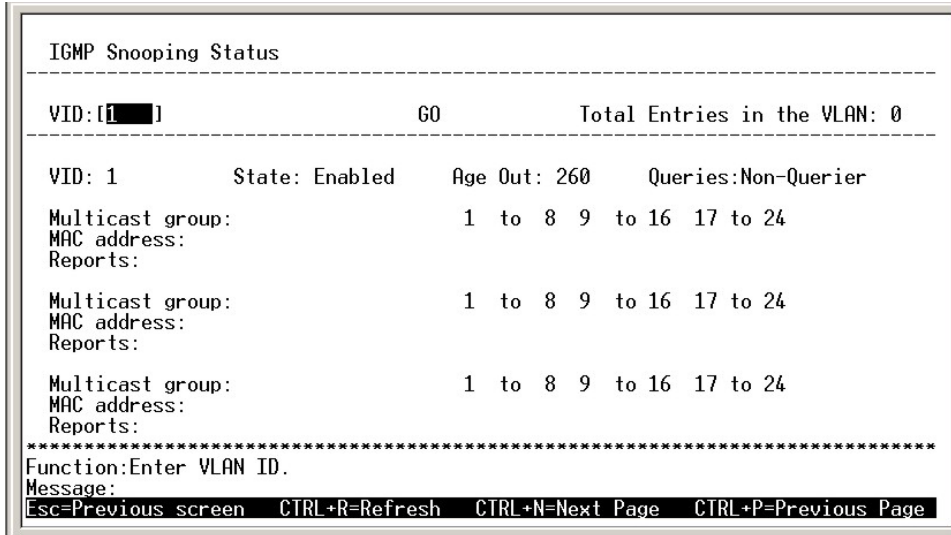


Figure 6-62. IGMP Snooping Status screen

Dynamic Group Registration Table

To view the **Dynamic Group Registration Table**, highlight **Dynamic Group Registration Table** on the **Network Monitoring Menu** and press **Enter**.

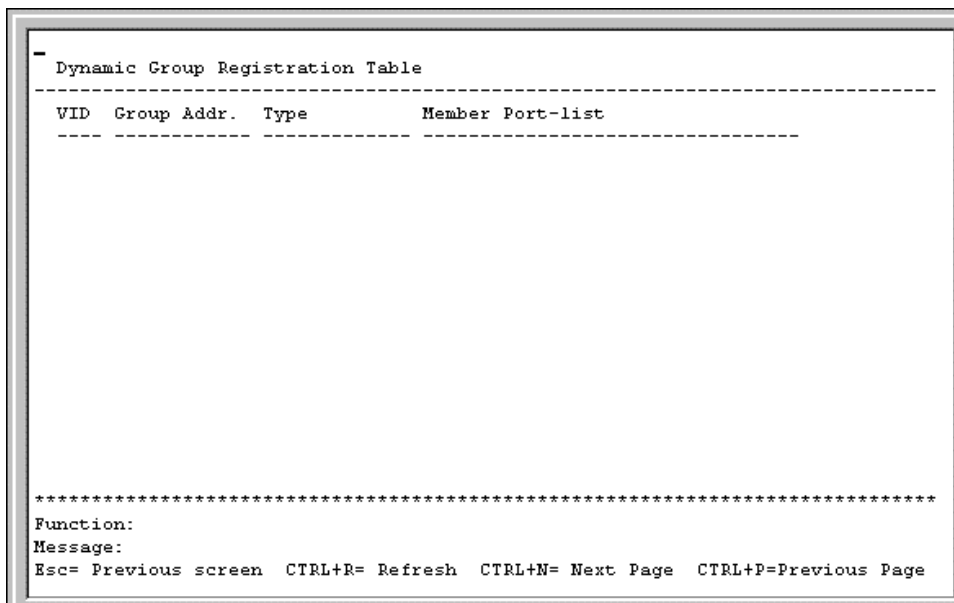


Figure 6-63. Dynamic Group Registration Table screen

This read-only table contains filtering information for VLANs configured into the bridge by (local or network) management, or learned dynamically, specifying the set of ports to which frames received on a VLAN for this FDB and containing a specific Group destination address are allowed to be forwarded.

VLAN Status

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

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

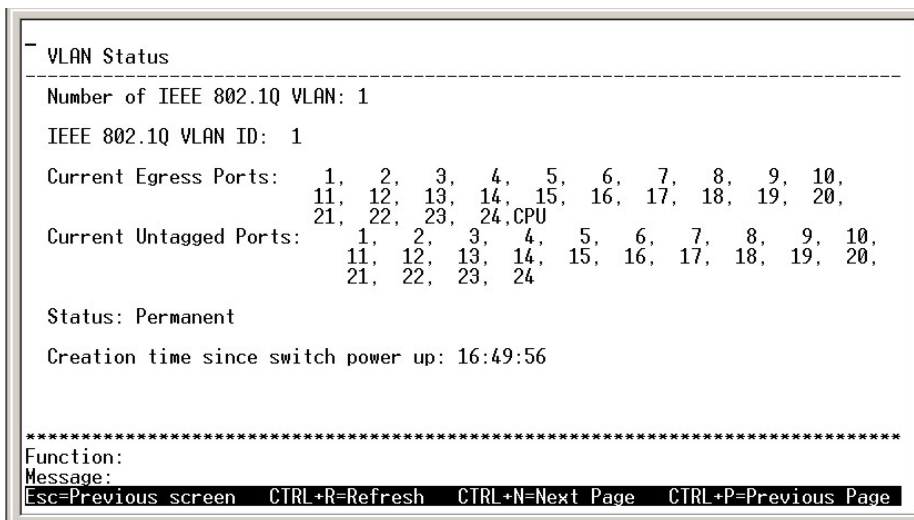


Figure 6-64. VLAN Status screen

Port Access Control Statistics

To view the **Monitor Authentication Statistics** menu, highlight **Port Access Control Statistics** on the **Network Monitoring Menu** and press Enter.

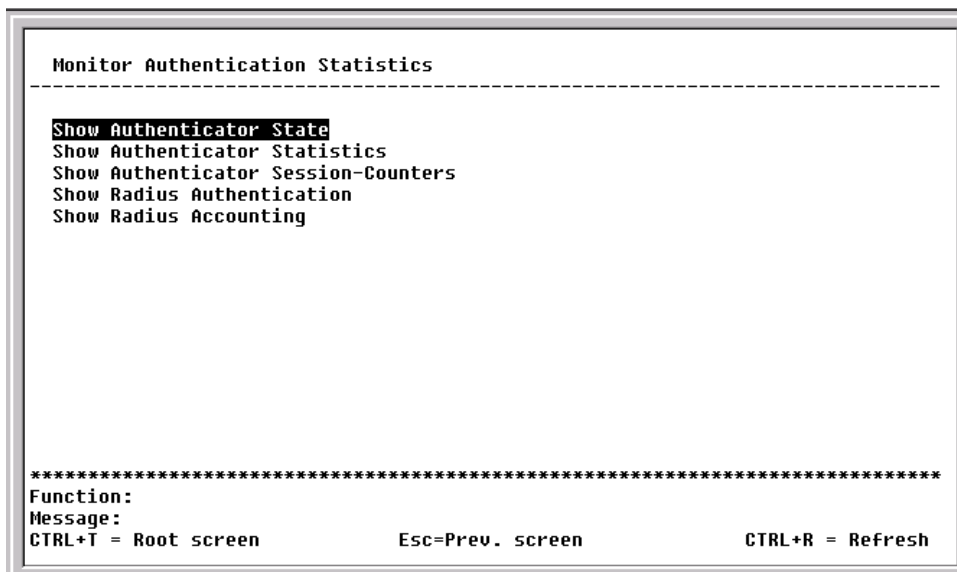


Figure 6-65. Monitor Authentication Statistics screen

Select the item from the screen above to show the desired information.

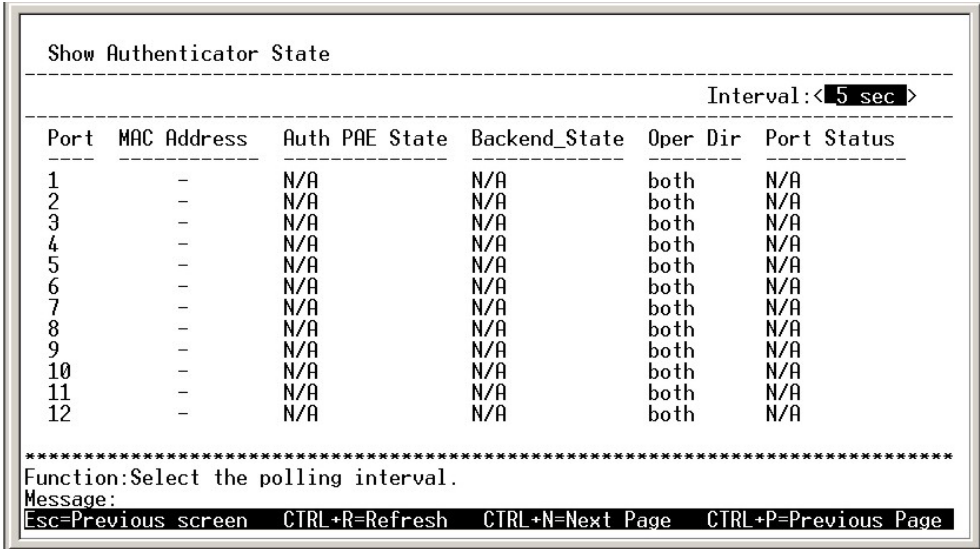


Figure 6-66. Show Authenticator State screen

This read-only field displays Authenticator State information. The polling interval can be set between 2 seconds and 1 minute using the space bar.

The information on this screen is described as follows:

AuthState – The Authenticator PAE state value can be: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth,* or *N/A*. *N/A* (Not Available) indicates that the port's authenticator capability is disabled.

BackendState – The Backend Authentication state can be *Request, Response, Success, Fail, Timeout, Idle, Initialize,* or *N/A*. *N/A* indicates that the port's authenticator capability is disabled.

AdmDir – Admin Controlled Directions can be either *both* or *in*.

OprDir – Oper Controlled Directions can be either *both* or *in*.

PortStatus – Auth Controlled Port Status can be *Authorized, Unauthorized,* or *N/A*.

Port Control – Auth Controlled Port Control can be *ForceAuthorized, ForceUnauthorized,* or *Auto*.

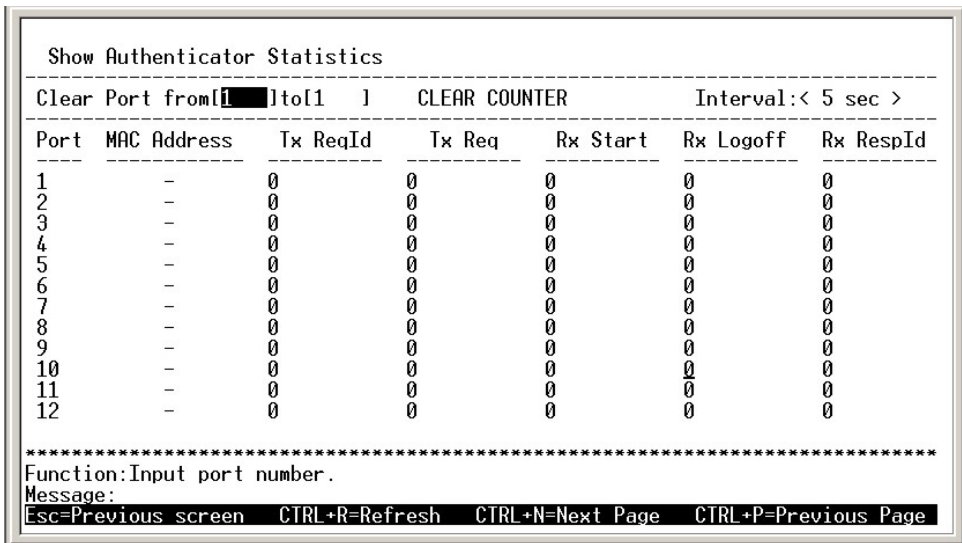


Figure 6-67. Show Authenticator Statistics screen

This read-only field displays Authenticator Statistics.

To reset the statistics counters on this screen, enter the desired ports in the **Clear Port from [] to []** field and then press CLEAR COUNTER. The polling interval can be set between 2 seconds and 1 minute using the space bar.

The information on this screen is described as follows:

- Tx ReqId** – The number of EAP Req/Id frames that have been transmitted by this Authenticator.
- Tx Req** – The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
- Rx Start** – The number of EAPOL Start frames that have been received by this Authenticator.
- Rx Logoff** – The number of EAPOL Logoff frames that have been received by this Authenticator.
- Rx RespId** – The number of EAP Resp/Id frames that have been received by this Authenticator.
- Rx Error** – The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.

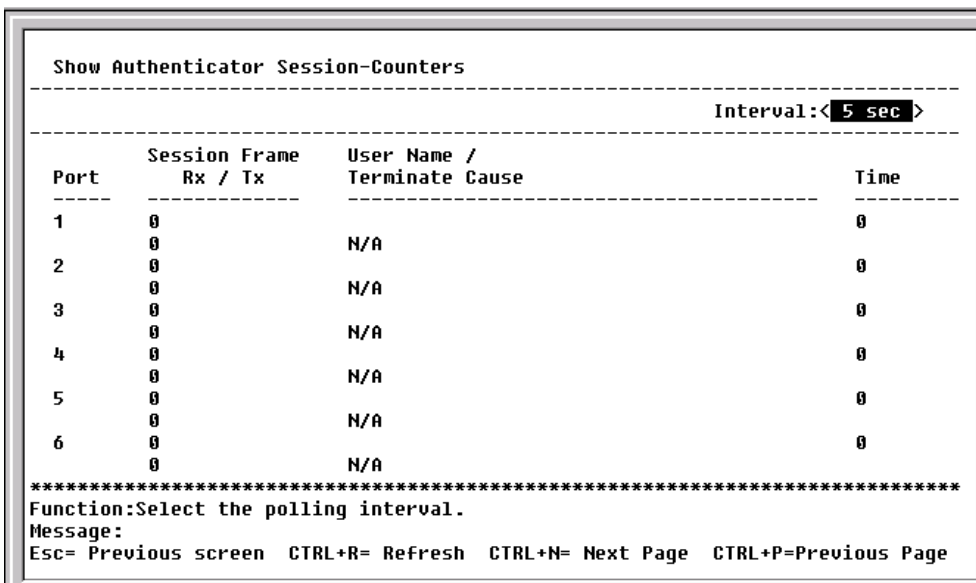


Figure 6-68. Show Authenticator Session-Counters screen

This read-only field displays Authenticator Session-Counters information. The polling interval can be set between 2 seconds and 1 minute using the space bar.

The information on this screen is described as follows:

- Session Frame Rx** – The number of user data frames received on this Port during the session.
- Session Frame Tx** – The number of user data frames transmitted on this Port during the session.
- User Name** – The User Name representing the identity of the client PAE.
- Terminate Cause** – The reason for the session termination. This parameter can take the following values: Client Logoff, Port Failure, Client Restart, Reauthentication Failure, AuthControlledPortControl set to ForceUnauthorized, Port Re-initialization, Port Administratively Disabled, and Not Terminated Yet.
- Time** – The session time is the duration of time in seconds.

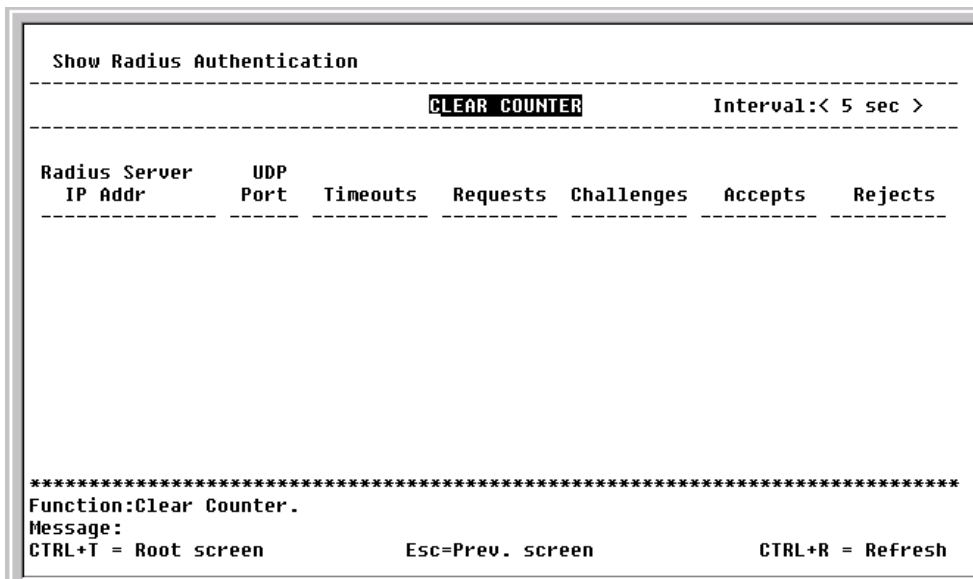


Figure 6-69. Show Radius Authentication screen

This read-only field displays RADIUS Authentication information. To reset the statistics counters on this screen, press CLEAR COUNTER. The polling interval can be set between 2 seconds and 1 minute using the space bar.

The information on this screen is described as follows:

- Radius Server IP Addr** – The remote RADIUS server IP address.
- UDP Port** – The UDP socket port numbers of the RADIUS server.
- Timeouts** – The counter of timeouts from RADIUS authentication.
- Requests** – The counter of access requests from RADIUS authentication.
- Challenges** – The counter of access challenges from RADIUS authentication.
- Accepts** – The counter for the number of acceptances from RADIUS authentication.
- Rejects** – The counter for the number of rejections from RADIUS authentication.

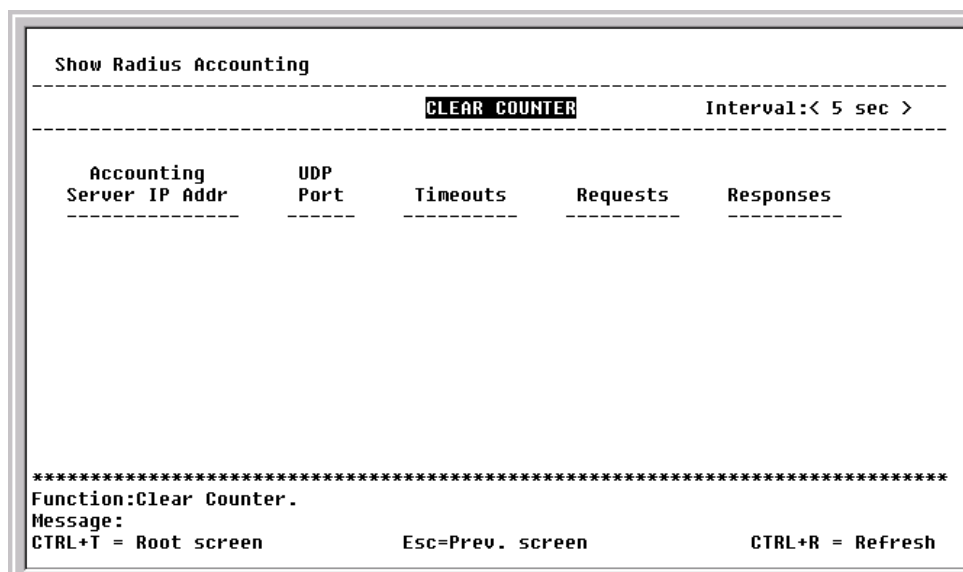


Figure 6-70. Show Radius Accounting screen

This read-only field displays RADIUS Accounting information. To reset the statistics counters on this screen, press CLEAR COUNTER. The polling interval can be set between 2 seconds and 1 minute using the space bar.

The information on this screen is described as follows:

Accounting Server IP Addr – The IP address of the RADIUS accounting server.

UDP Port – The UDP socket port number of the RADIUS accounting server.

Timeouts – The counter of the timeout connections to the RADIUS accounting server.

Requests – The counter of the requests from the RADIUS accounting server.

Responses – The counter for the number of rejections from RADIUS accounting server.

SNMP Manager Configuration

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 DView.

SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol.
- Collecting information about the status and current configuration of network devices.
- Modifying the configuration of network devices.

The DES-3210/DES-3218/DES-3226 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.

SNMP V1 & V2

SNMP V1/V2 implements a rudimentary form of security by requiring that each request include a *community name*. A community name is an arbitrary string of characters used as a "password" to control access to the Switch. If the Switch receives a request with a community name it does not recognize, it will trigger an authentication trap.

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

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

Choose **SNMP Manager Configuration** under the **Main Menu** to access the following screen:

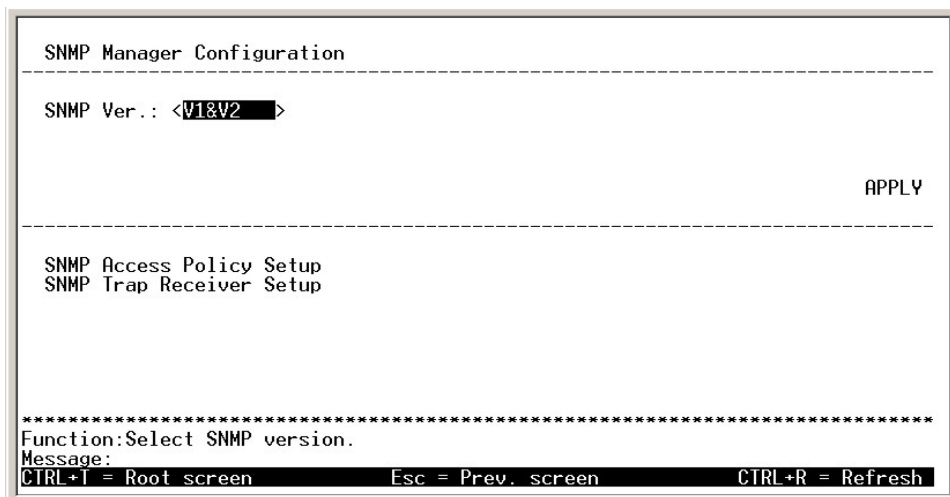


Figure 6- 71. SNMP Manager Configuration screen

SNMP Access Policy Setup

To access the following screen, highlight **SNMP Access Policy Setup** and press Enter.

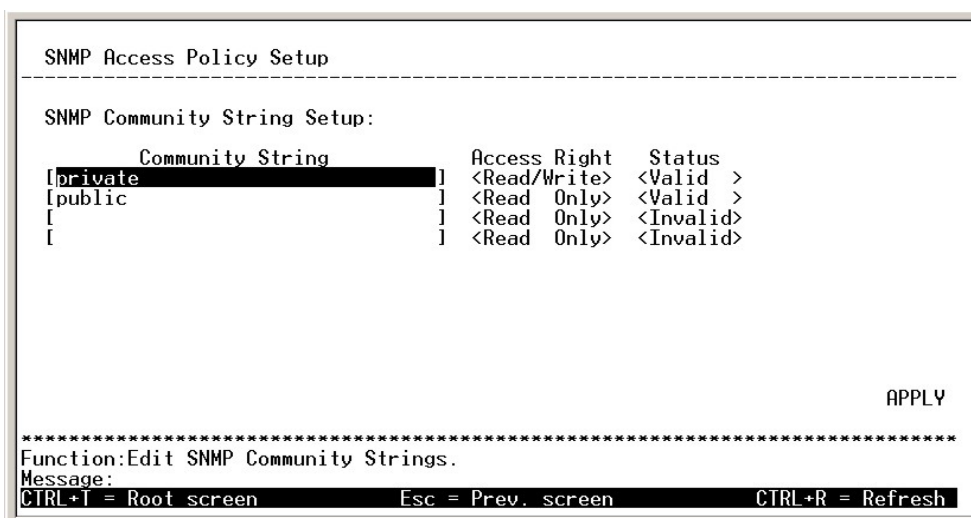


Figure 6- 72. SNMP Access Policy Setup screen

The following fields can be set:

SNMP Community String – The community string that will be included on SNMP packets sent to and from the switch. A station not privy to this community will not receive the packet.

Access Right – Allows each community to be separately set to either *Read Only*, meaning that the community member can only view switch settings or *Read/Write*, which allows the member to change settings in the switch.

Status – Determines whether this community name entry is *Valid* or *Invalid*. An entry can be disabled by changing its status to *Invalid*.

SNMP Trap Receiver Setup

To access the following screen, highlight **SNMP Trap Receiver Setup** and press Enter.

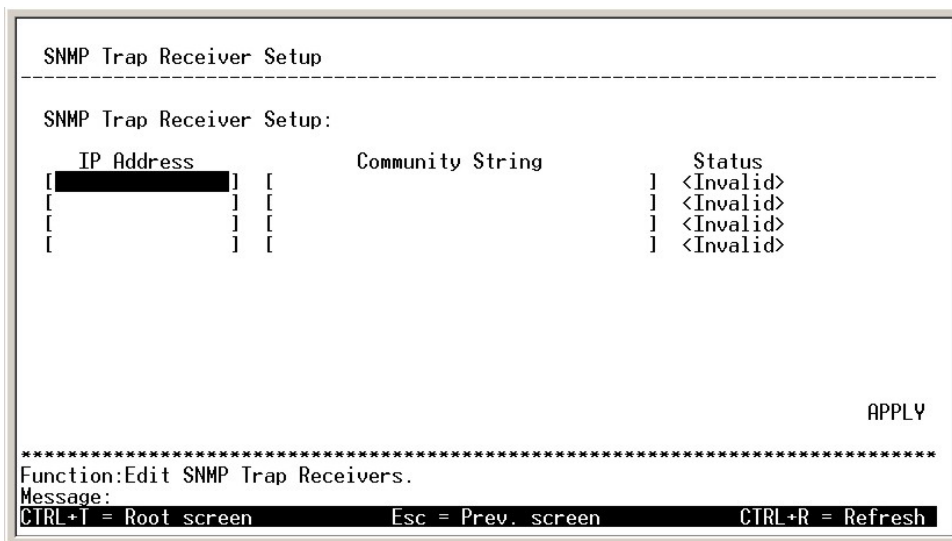


Figure 6- 73. SNMP Trap Receiver Setup screen

The following fields can be set:

IP Address – The IP address of the network management station to receive traps.

SNMP Community String – The community string that will be included on SNMP packets sent to and from the switch. A station not privy to this community will not receive the packet.

Status – Determines whether this community name entry is *Valid* or *Invalid*. An entry can be disabled by changing its status to *Invalid*.

SNMP V3

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. One part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMP v1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v3.

Using SNMP v3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB.

An additional layer of security is available for SNMP v3 in that SNMP messages may be encrypted (using HMAC-SHA-96 or HMAC-MDA-96 authentication levels).

To access **SNMP V3**, toggle the SNMP Ver. under the **SNMP Manager Configuration** to *V1&V2&V3*, highlight **APPLY** and press Enter. If the user wishes to modify the Engine ID number, toggle the Modify ID setting to *Yes* and enter the ID into the NEW ID field.

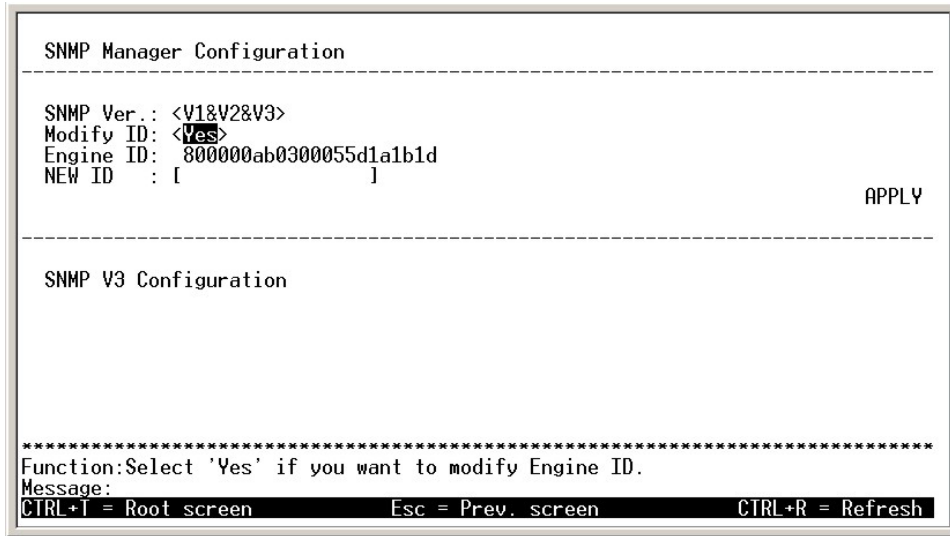


Figure 6- 74. SNMP Manager Configuration screen

Highlight **SNMP V3 Configuration** and press Enter, revealing the following menu:

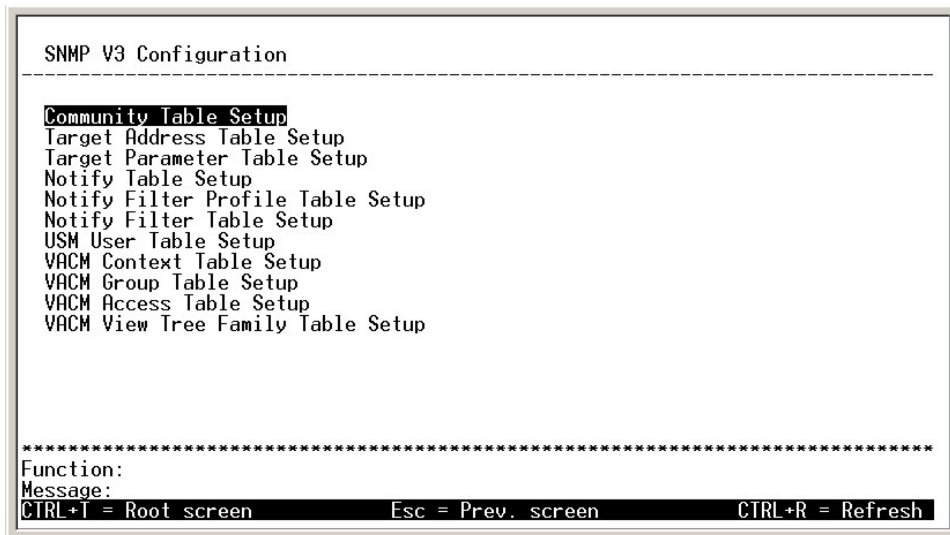


Figure 6- 75. SNMP V3 Configuration menu

This menu offers eleven setup screens for configuring SNMP V3 on the switch, including Community Table Setup, Target Address Table Setup, Target Parameter Table setup, Notify Table Setup, Notify Filter Profile Table Setup, Notify Filter Table Setup, USM User Table Setup, VACM Context Table Setup, VACM Group Table Setup, VACM Access Table Setup and VACM View Tree Family Table Setup.

Community Table Setup

Highlight **Community Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

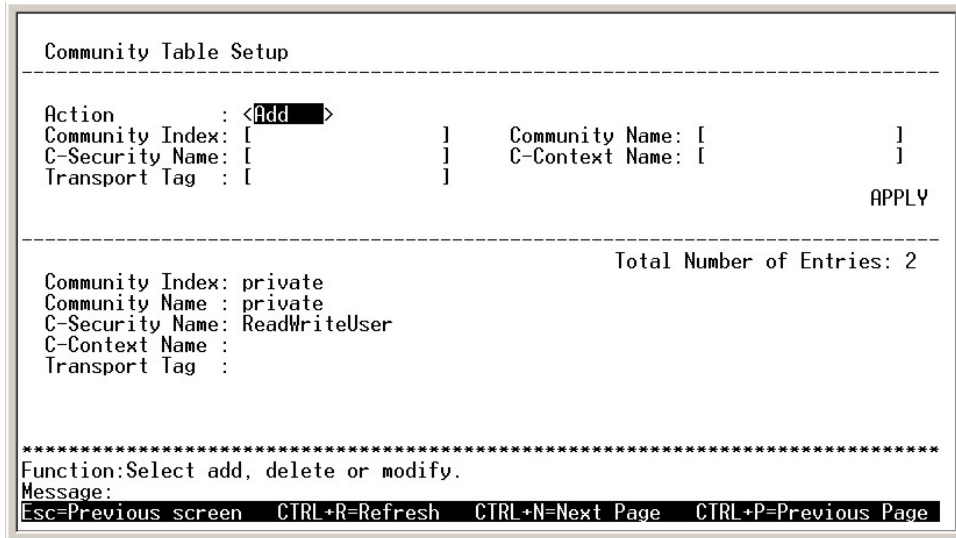


Figure 6- 76. Community Table Setup screen

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.
- ReadWriteUser or ReadOnly level permission for the MIB objects accessible to the SNMP community.

To change a community string, configure the following fields:

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user's intentions.

Community Index: [] – 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.

Community Name: [] – Type an alphanumeric string of up to 32 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.

C-Security Name: [] – ReadOnly – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch.

– ReadWriteUser – 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.

C-Context Name: [] – This is the value originally determined for the notification.

Transport Tag: [] – Enter a value to use to select entries in the Target Address Table. Any entry in the Target Address Table that contains a tag value that is equal to the value of the object selected. If this object is nil, no entries are selected.

Target Address Table Setup

The Target Address Table Setup contains addresses of the targets for notifications (also under this menu). It also contains information for establishing the transport parameters.

Highlight **Target Address Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

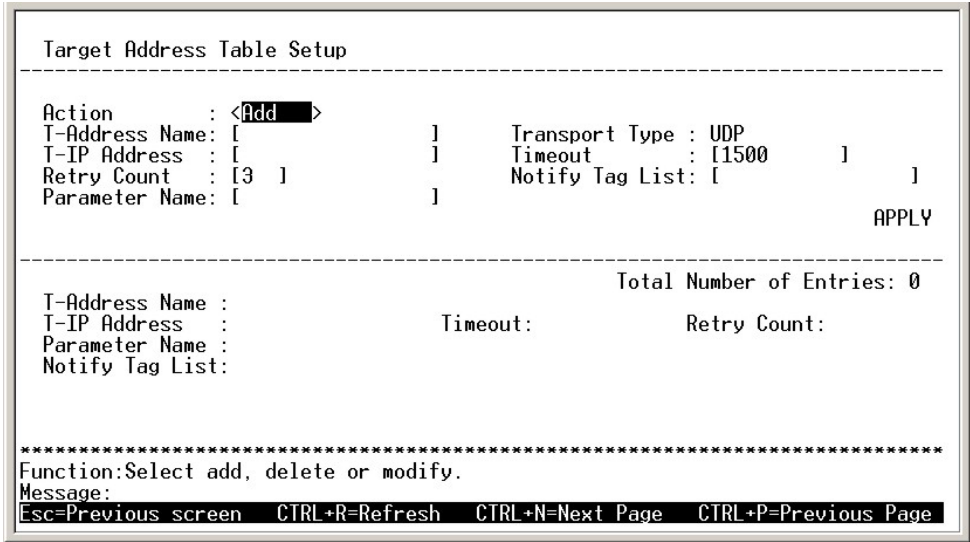


Figure 6- 77. Target Address Table Setup screen

To configure a Target Address, modify the following fields and press APPLY.

- Action:**<Add> – May be toggled to Add, Modify or Delete depending on the user’s intentions.
- T-Address Name:** [] – Enter an alphanumeric string of up to 32 characters that is used to name the target address.
- Transport Type:** UDP – This field shows the system used to transport the notifications, which is UDP (User Datagram Protocol).
- T-IP Address:** [] – Enter the IP address that you would like to target.
- Timeout:** [1500] – Enter the time, in seconds, that the switch will wait for a response to an inform notification before resending that notification.
- Retry Count:** [3] – Enter the number of retries to be attempted when a response is not received for a generated message. The default setting is 3.
- Notify Tag List:** [] – Enter the space separated list of tag values to be used to select target addresses for a particular procedure.
- Parameter Name:** [] – Enter a numeric string to identify an entry in the SNMP Parameter Table . The identified entry contains SNMP parameters to be used when generated messages are sent to this transport address.

Target Parameter Table Setup

SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients. You can view a table of existing SNMPv3 target parameter configurations, create SNMPv3 target parameters that associate notifications with particular recipients, and delete existing SNMPv3 target parameter configurations.

Highlight **Target Parameter Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

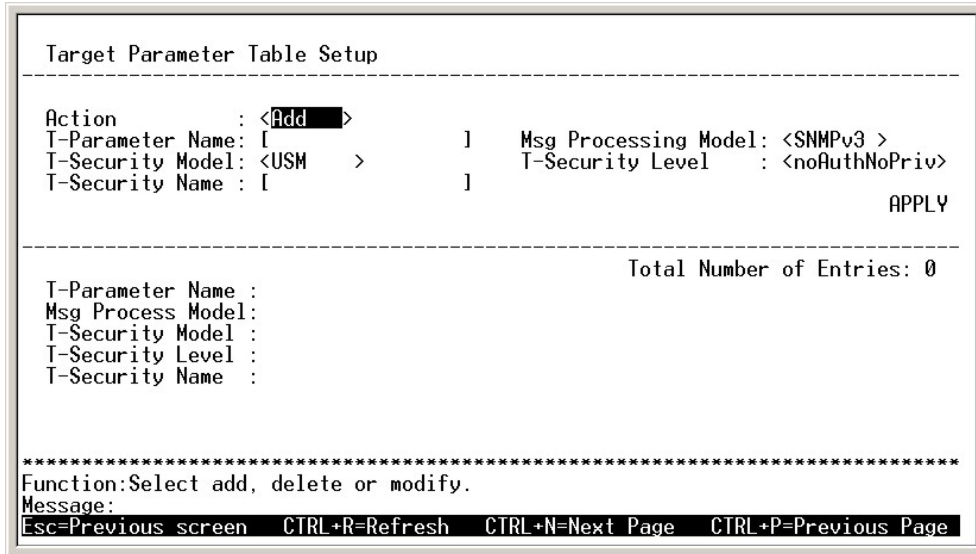


Figure 6- 78. Target Parameter Table Setup screen

To configure a Target Parameter, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user’s intentions.

T-Parameter Name: [] – Enter an alphanumeric string of up to 32 characters to identify the parameter name.

Msg Processing Mode: <SNMPv3> – Choose the message-processing model to be used when generating SNMP messages for this entry. This field may be toggled between SNMPv1, SNMPv2 and SNMPv3.

T-Security Model: <USM> – This field indicates the security model used to generate the message. The user may toggle between *SNMPv1*, *SNMPv2* and *USM*. The SNMPv3 standard recommends the use of USM security model.

T-Security Level: <noAuthNoPriv> – Choose the level of security to be used when generating SNMP messages, using this entry. This field may be toggled between noAuthNoPriv, authNoPriv and authPriv.

T-Security Name: Enter the principal, on whose behalf SNMP messages are generated, using this entry.

Notify Table Setup

Notify table contains groups of management targets to receive notifications and the type of notifications. The target addresses to receive notifications that are listed in target address table (see target group) are tagged here.

Highlight **Notify Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

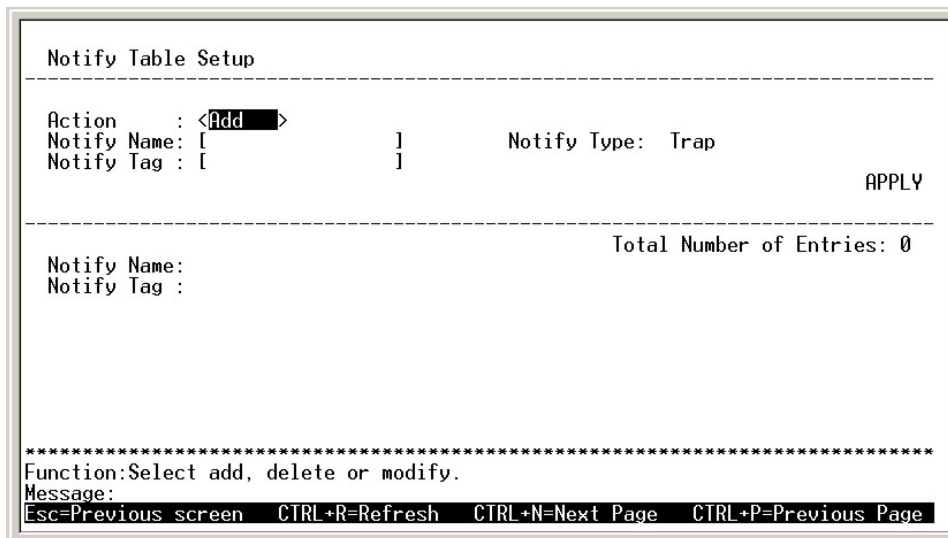


Figure 6- 79. Notify Table Setup screen

To configure the **Notify Table Setup**, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user’s intentions.

Notify Name: [] – Enter an alphanumeric string of up to 32 characters as a unique identifier used to index the Notify Table.

Notify Type: Trap – Type of notification to be used. On this switch, it is set at *Trap* which can not be altered.

Notify Tag: [] – Enter an alphanumeric string of up to 32 characters to name the entry in the Notify Table.

Notify Filter Profile Table Setup

This table is used to associate a notification filter profile with a particular set of target parameters.

Highlight **Notify Filter Profile Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

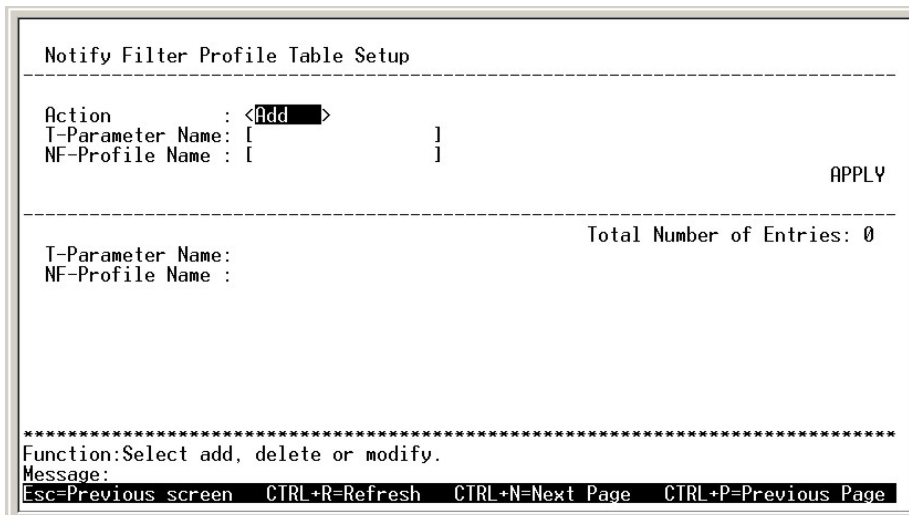


Figure 6- 80. Notify Filter Profile Table Setup screen

To configure the **Notify Filter Profile Table Setup**, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user’s intentions.

T-Parameter Name: [] – Enter an alphanumeric string of up to 32 characters indicating the name of the filter profile to be used when generating notifications using the corresponding entry in the Target Parameter Table. The name of the filter profile to be used when generating notifications using the corresponding entry in the Target Address Table.

NF-Profile Name: [] – Enter an alphanumeric string of up to 32 characters indicating the name of the filter profile to be used when generating notifications using the corresponding entry in the Target Address Table.

Notify Filter Table Setup

This is a table of filter profiles. Filter profiles are used to determine whether particular management targets should receive particular notifications. When a notification is generated, it must be compared with the filters associated with each management target that is configured to receive notifications. If the notification is matched by a filter, it is not sent to the management target with which the filter is associated.

Highlight **Notify Filter Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

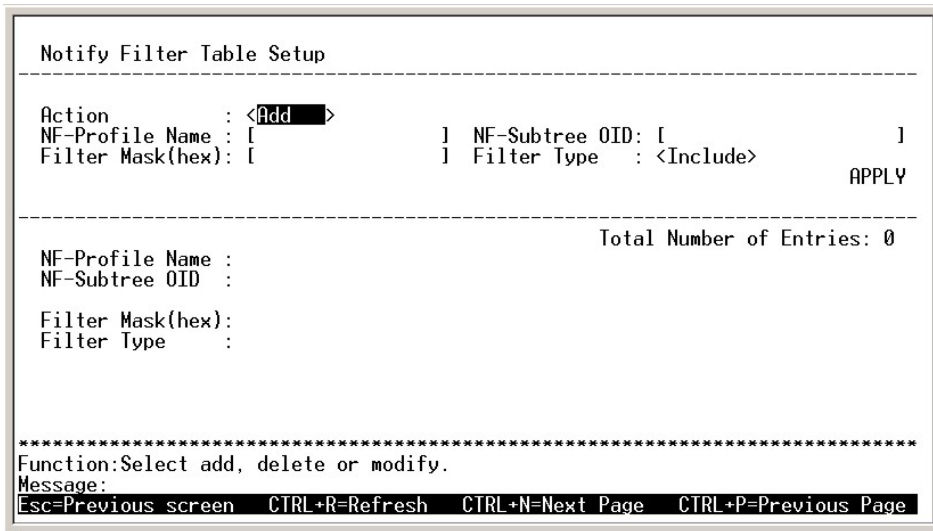


Figure 6- 81. Notify Filter Table Setup screen

To configure the **Notify Filter Table Setup**, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user’s intentions.

NF-Profile Name: [] – Enter the alphanumeric string of up to 32 characters indicating the name of the filter profile to be used when generating notifications using the corresponding entry in the Target Address Table, corresponding to the identical entry in the previous screen.

NF-Subtree OID: [] – Enter the alphanumeric string of up to 32 characters indicating the MIB subtree which, when combined with the corresponding instance of the Filter Mask, defines a family of subtrees which are included in or excluded from the filter profile.

Filter Mask (hex): [] – Enter the alphanumeric string of up to 32 characters indicating the bit mask which, in combination with the corresponding instance of the Filter Subtree, defines a family of subtrees which are included in or excluded from the filter profile.

Filter Type: <Include> –Toggle between *Include* and *Exclude* to indicate whether the family of filter subtrees defined by this entry are included in or excluded from a filter.

USM User Table Setup

The USM Setting Table allows the administrator to define new user names and associated security information.

Highlight **USM User Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

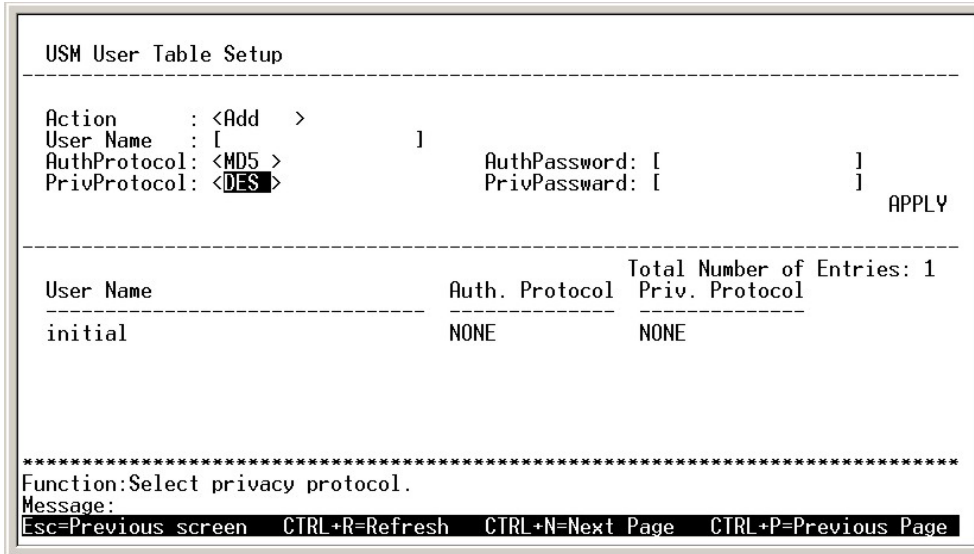


Figure 6- 82. USM User Table Setup screen

To configure the **Notify Filter Table Setup**, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user's intentions.

User Name: [] – Enter the alphanumeric string of up to 32 characters indicating the textual name of a user.

AuthProtocol: <NONE> – Toggle between NONE, MD5 or SHA1 to choose the Authentication Protocol. Indicating a protocol will automatically prompt for a password.

AuthPassword: [] – Enter the password used as part of the authentication process. The password is automatically manipulated to conform to the specific requirements of the specific authentication protocol. If no authentication protocol is selected, you do not need a password.

PrivProtocol: <NONE> – Toggle Between NONE and DES to choose the Privacy Protocol. Indicating a protocol will automatically prompt for a password.

PrivPassword: [] – Enter the password used as part of the privacy process. The password is automatically manipulated to conform to the specific requirements of the specific privacy protocol. If no privacy protocol is selected, you do not need a password.

VACM Context Table Setup

View-based Access Control Model (VACM) is a default access control model defined by SNMPv3 frame work. The SNMPv3 agent has implemented the VACM MIB as a default access control model.

Here is a set of valid context names supported by the SNMPv3 agent. The received context name will be checked with this table in the access validation phase

Highlight **VACM Context Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

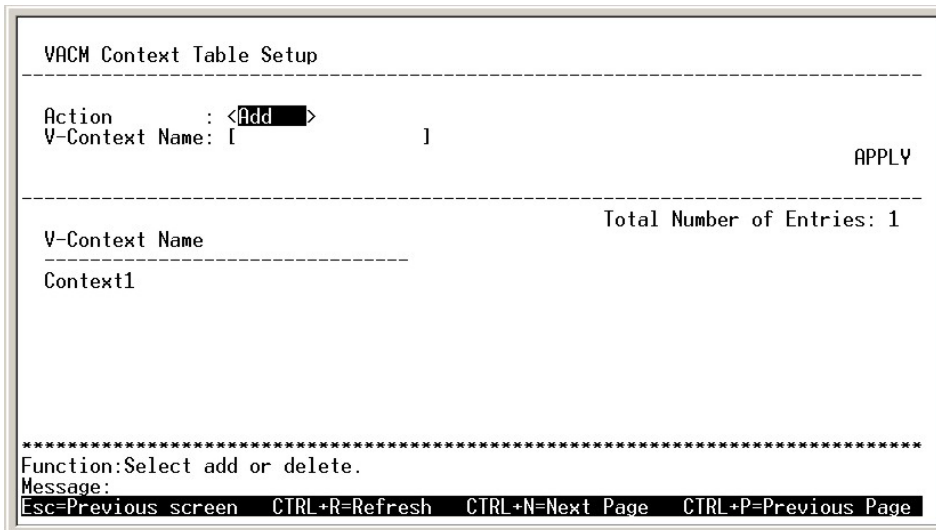


Figure 6- 83. VACM Context Table Setup screen

To configure the **VACM Context Table Setup**, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user’s intentions.

V-Context Name: [] –The context names supported by the SNMPv3 agent. The received context name will be checked with this table in the access validation phase. Leaving the field empty (zero length) represents the default context.

VACM Group Table Setup

This table maps a combination of security model and security name into a group name that is used to define an access control policy for a group of principals.

Highlight **VACM Group Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

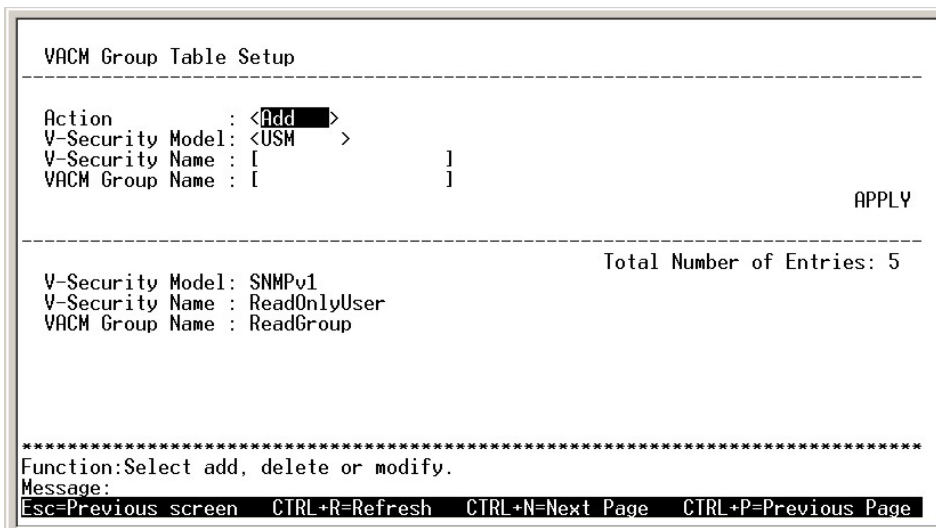


Figure 6- 84. VACM Group Table Setup screen

To configure the **VACM Group Table Setup**, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user’s intentions.

V-Security Model: <USM> – Toggle between *USM*, *SNMPv1* or *SNMPv2c* to map the combination of a security model and security name into a group name.

V-Security Name: [] – Enter the alphanumeric string of up to 32 characters indicating the security name for the principal, represented in a security model independent format, which is mapped by this entry to a group name.

VACM Group Name: [] – Enter the alphanumeric string of up to 32 characters indicating the name of the group to which this entry (e.g., the combination of security model and security name) belongs. This group name is used as index into the VACM Access Table Setup to select an access control policy.

VACM Access Table Setup

The VACM Access Table Setup is a table of access rights for groups. Each entry is indexed by a context prefix, a group name, a security model and a security level. To determine whether access is allowed, one entry from this table needs to be selected and the proper view name from that entry must be used for access control checking.

Highlight **VACM Access Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

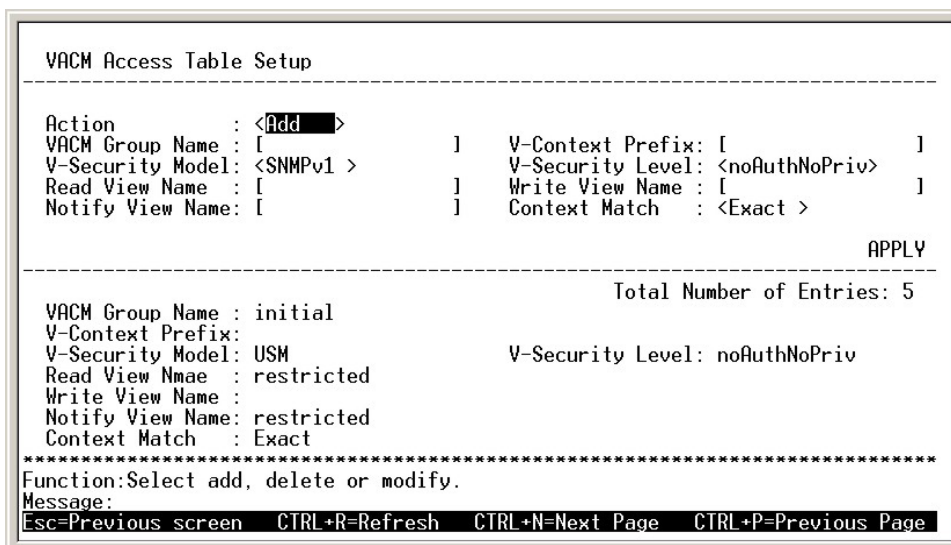


Figure 6- 85. VACM Access Table Setup screen

To configure the **VACM Access Table Setup**, modify the following fields and press APPLY.

Action:<Add> – May be toggled to Add, Modify or Delete depending on the user's intentions.

VACM Group Name: [] – Enter the name of the group which was entered in the same field in the previous screen.

V-Context Prefix: [] – In order to gain the access rights allowed by this conceptual row, a context name entered must match exactly (if the value of VACM Access Context Match is 'exact') or partially (if the value of VACM Access Context Match is 'prefix') to the value of the instance of this object.

V-Security Model: < SNMPv1 > –Toggle between USM, SNMPv1 or SNMPv2c order to gain the access rights allowed by this conceptual row.

V-Security Level: <noAuthNoPriv> – Toggle between noAuthNoPriv, authNoPriv, or authPriv to enable the minimum level of security required in order to gain the access rights allowed by this conceptual row.

Read View Name: [] –Enter the value of this object that identifies the MIB view of the SNMP context to which this conceptual row authorizes read access.

Write View Name: [] – Enter the value of this object identifying the MIB view of the SNMP context to which this conceptual row authorizes write access.

Notify View Name: [] –Enter the value of this object identifying the MIB view of the SNMP context to which this conceptual row authorizes access for notifications.

Context Match: <Exact> Toggle between *Exact* and *Prefix*. If the value of this object is exact, then all rows where the context name exactly matches VACM Access Context Prefix are selected. If the value of this object is prefix, then all rows where the context name whose starting octets exactly match VACM Access Context Prefix are selected. This allows for a simple form of wildcarding.

VACM View Tree Family Table Setup

This screen allows the user to alter the locally held information about families of subtrees within MIB views.

Each MIB view is defined by two sets of view subtrees:

- the included view subtrees, and
- the excluded view subtrees.

Every such view subtree, both the included and the excluded ones, is defined in this table.

Highlight **VACM View Tree Family Table Setup** from the **SNMP V3 Configuration** menu and press Enter:

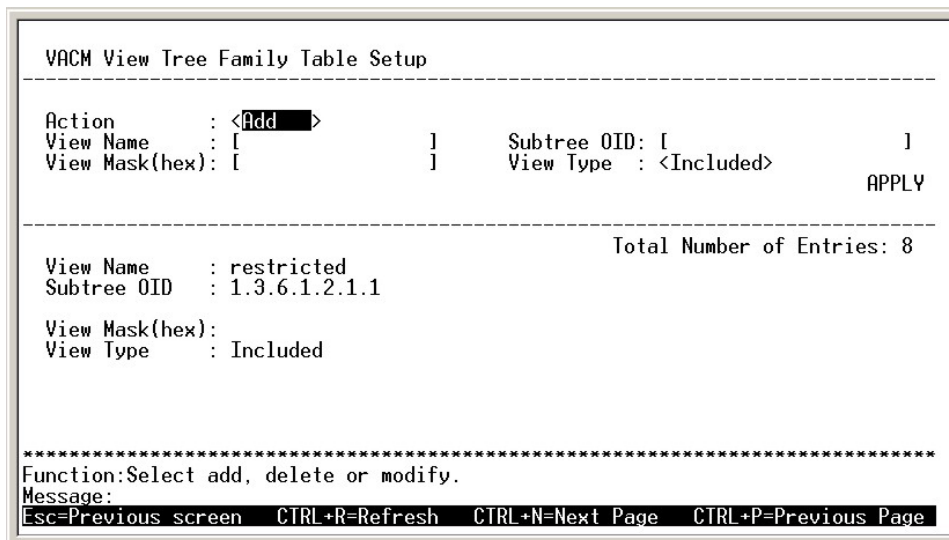


Figure 6- 86. VACM View Tree Family Table Setup screen

To configure the **VACM View Family Tree Setup**, modify the following fields and press **APPLY**.

Action: <Add> – May be toggled to Add, Modify or Delete depending on the user's intentions.

View Name: [] – Enter an alphanumeric string of up to 32 characters indicating the name for a family of view subtrees.

Subtree OID: [] – Enter an alphanumeric string of up to 32 characters indicating the MIB subtree which when combined with the corresponding VACM View Tree Family Mask, defines a family of view subtrees.

View Mask (hex): – Enter the bit mask, which, in combination with the corresponding VACM View Tree Family Subtree, defines a family of view subtrees.

View Type: <Included> – Toggle between *Included* or *Excluded* to indicate whether the corresponding instances of VACM View Tree Family Subtree and VACM View Tree Family Mask define a family of view subtrees will be included in or excluded from the MIB view.

System Utilities

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

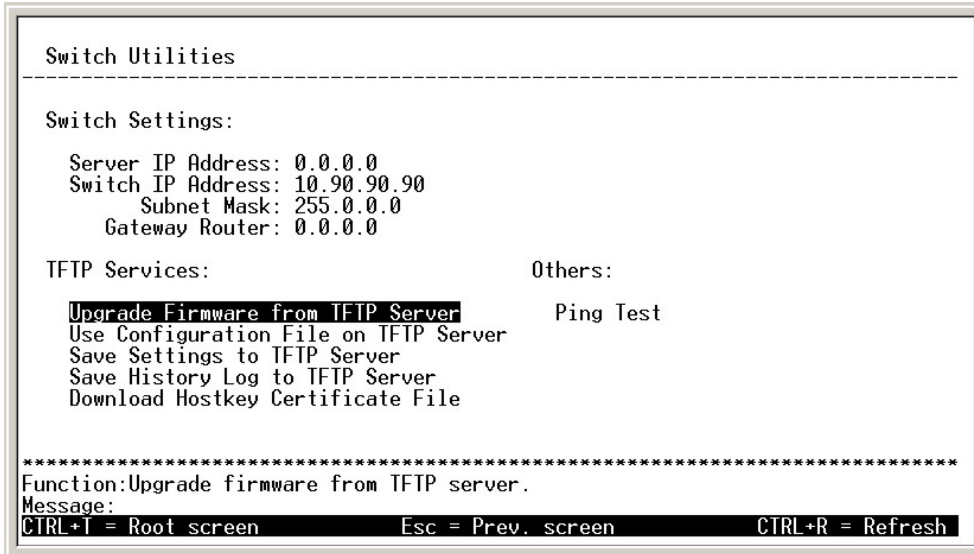


Figure 6-87. Switch Utilities menu

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

Upgrade Firmware from TFTP Server

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

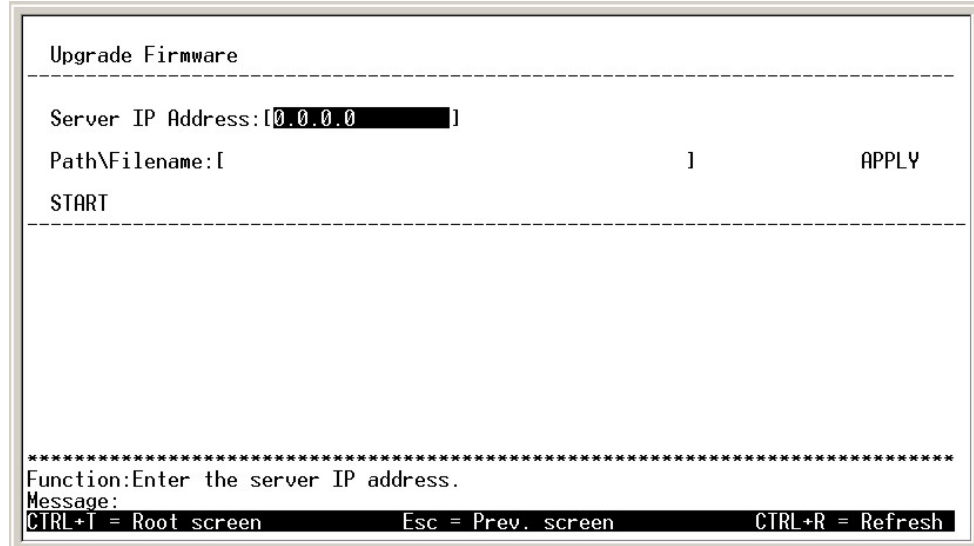


Figure 6-88. Upgrade Firmware screen

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

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

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

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

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

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

Use Configuration File on TFTP Server

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

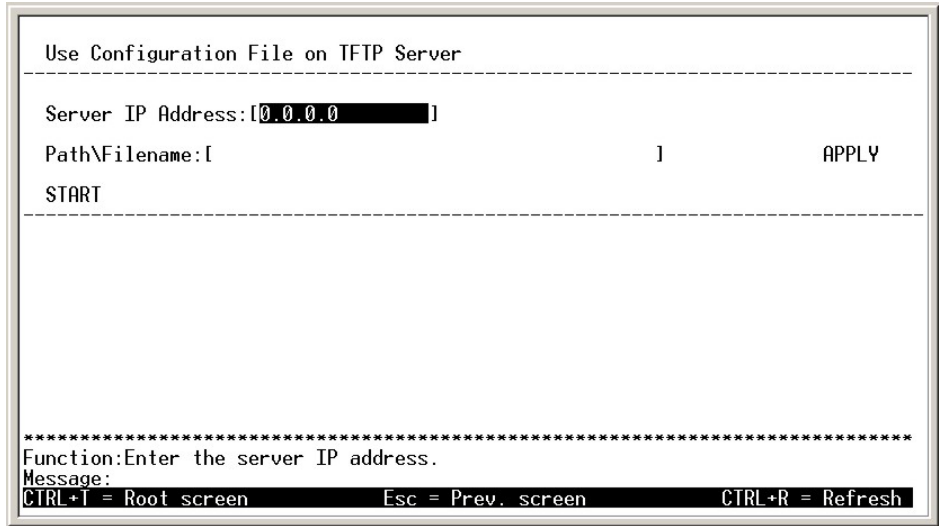


Figure 6-89. Use Configuration File on TFTP Server screen

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

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

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

Note: Configuration files used in the earlier version of this switch (firmware version 1.0) are not supported by the present version (firmware version 2.0). The Switch Information screen displays the firmware version.

Save Settings to TFTP Server

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

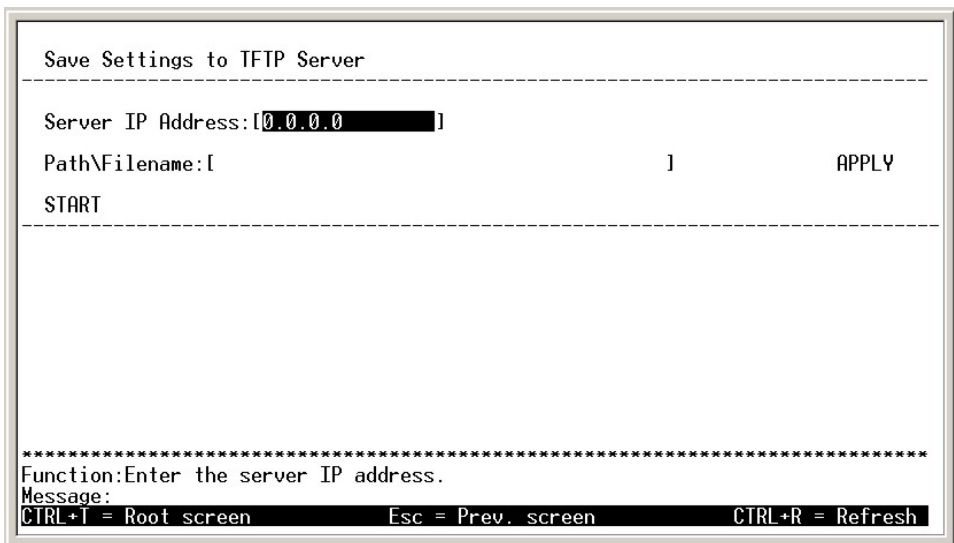


Figure 6-90. Save Settings to TFTP Server screen

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

Save History Log to TFTP Server

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

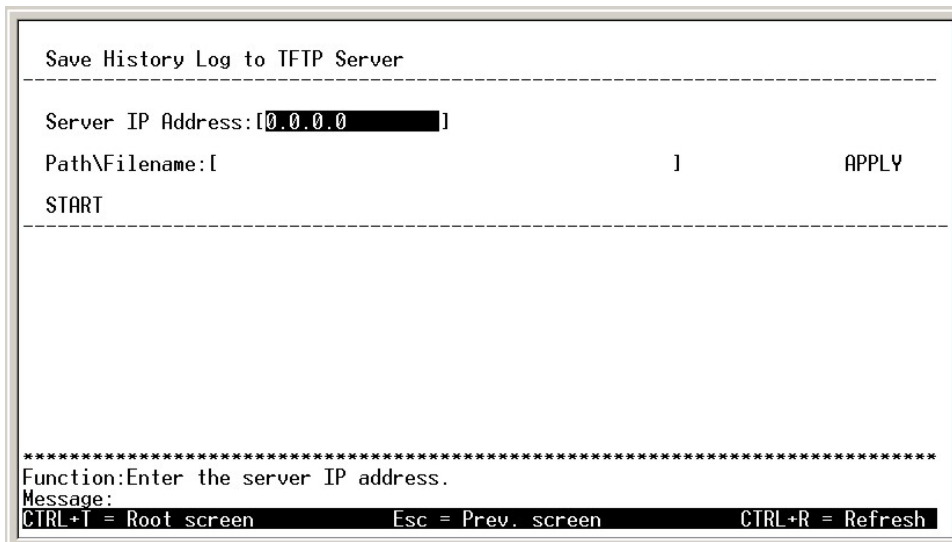


Figure 6-91. Save Log to TFTP Server screen

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

Download Hostkey Certificate File

To download the Hostkey Certificate File for the Security Shell (SSH), highlight **Download Hostkey Certificate File** and press Enter.

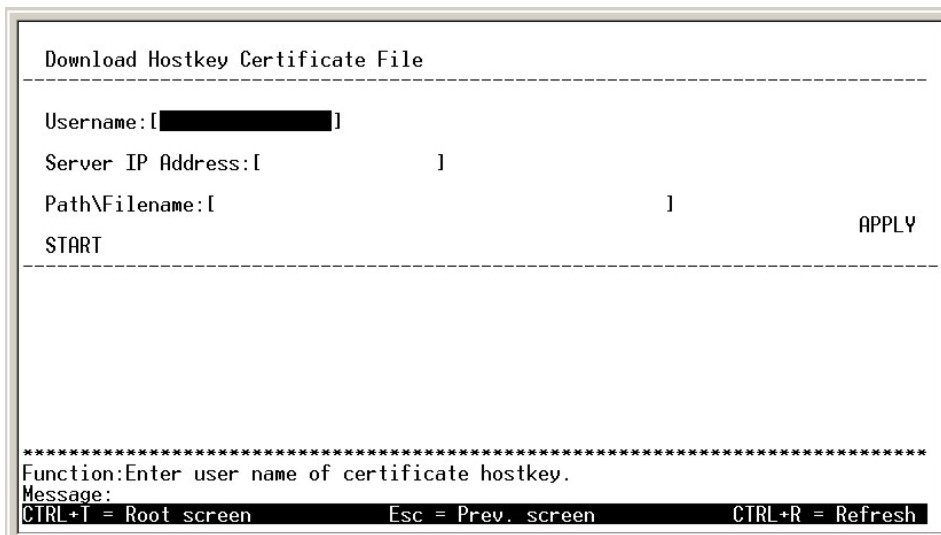


Figure 6-92. Download Hostkey Certificate File screen

To download the Hostkey Certificate file, modify the following fields and press APPLY and then START.

Username: [] – Enter the username that was applied in the SSH (Security Shell) settings.

Server IP Address: [] – Enter the IP address of the server where the file is being downloaded from.

Path\Filename: [] – Enter the name of the path to be downloaded. Note that the file must be a .cer file.

Highlight **APPLY** and press **Enter** to make the changes current. Highlight **START** and press **Enter** to initiate the file transfer.

Ping Test

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

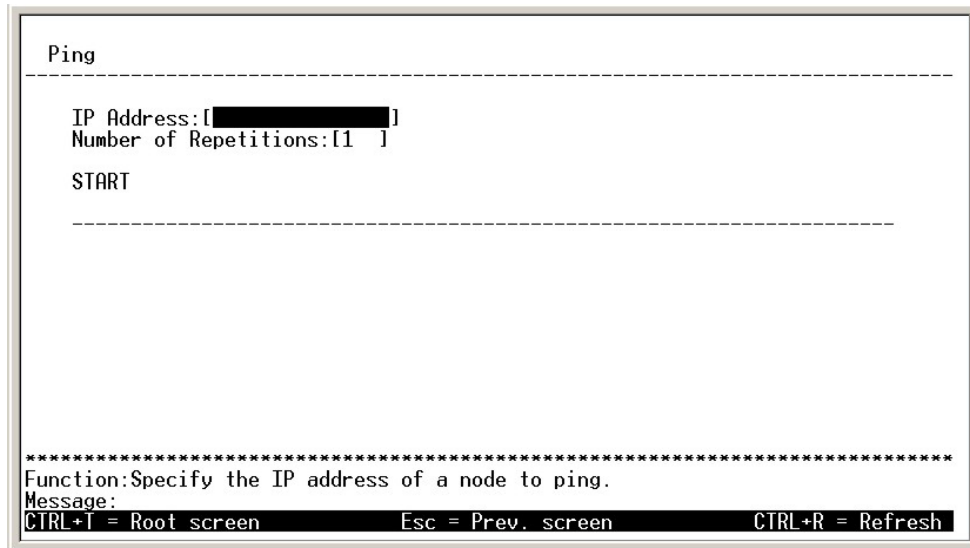


Figure 6-93. Ping screen

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

Reboot

The DES-3210/DES-3218/DES-3226 has several reboot options.

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

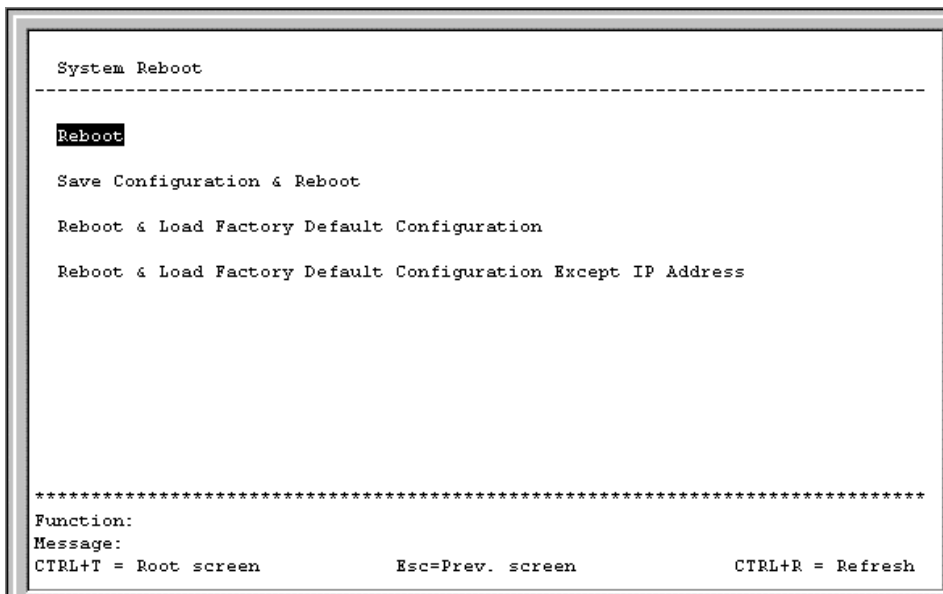


Figure 6-94. System Reboot menu

The reboot options are as follows:

Reboot – Simply restarts the Switch. Any configuration settings not saved using **Save Changes** from the main menu will be lost. The Switch's configuration will be restored to the last configuration saved in NV-RAM.

Save Configuration & Reboot – Saves the configuration to NV-RAM (identical to using **Save Changes**) and then restarts the Switch.

Reboot & Load Factory Default Configuration – Restarts the Switch using the default factory configuration. All configuration data will be lost. This is identical to using **Factory Reset** and then **Reboot**.

Reboot & Load Factory Default Configuration Except IP Address – Restarts the Switch using the default factory configuration, except the user configured IP address will be retained. All other configuration data will be lost.

A confirmation screen will appear:

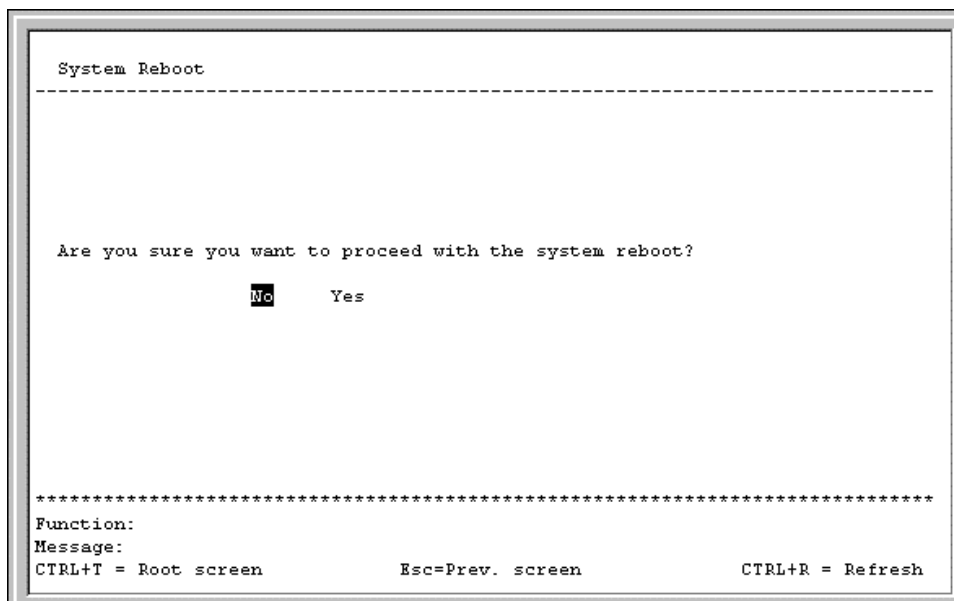


Figure 6-95. System Reboot confirmation screen

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

WEB-BASED NETWORK MANAGEMENT

Introduction

The DES-3210/DES-3218/DES-3226 offers an embedded Web-based (HTML) interface allowing users to manage the Switch from anywhere on the network through a standard browser, such as Opera, Netscape Navigator/Communicator, or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol. Your browser window may vary with the screen shots (pictures) in this guide.

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

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

Getting Started

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

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

You are now ready to begin managing your Switch by simply running the browser installed on your computer and pointing it to the IP address you have defined for the device. The URL in the address bar should read something like:

http://123.123.123.123, where the numbers 123 represent the IP address of the switch. Please note that the proxy for session connection should be turned off.

The following dialog box will open:

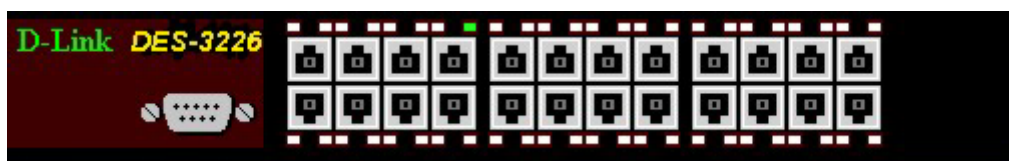


Click **OK** as there is no preset user name or password on the Switch. This opens the main page in the management module. The panel on the left-hand side contains the main menu. The featured items include: **Configuration**, **Security Management**, **User Account Manager**, **SNMP Manager**, **Monitoring**, **Maintenance**, and **Help**.



These are the major categories for Switch management. Clicking on the small square hyperlink to the left of the folder icons will cause a list of additional sub-menus to appear directly below each of the first four main menu categories.

The top panel on the right-hand side contains a real-time front panel display of the Switch. Double-clicking on a port will open the Rx Packets Analysis window. This can also be accessed through **Monitoring** → **Packets** → **Received (RX)**. Please see the Monitoring section in this chapter for a detailed description.



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

Configuration

The first category includes: IP Address, Switch Information, Advanced Settings, Port Configuration, Port Mirroring, Port LACP Trunking, IGMP Snooping, Port GMRP, Diffserv Settings, Spanning Tree, Static Filtering Table, VLANs, Port Bandwidth, Threshold of Broadcast, Port Bandwidth and QoS, as well secondary screens.

IP Address

Switch IP Setting	
MAC Address	00:10:27:32:26:b1
Get IP From	Manual <input type="button" value="v"/>
IP Address	10.53.13.212
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
VID	1
<input type="button" value="Apply"/>	

Figure 7-1. TCP/IP Parameters Setup window

This window is used to determine whether the Switch should get its IP Address settings from the user (*Manual*), a *BOOTP* server, or a *DHCP* server. If you are not using either BOOTP or DHCP, enter the **IP Address**, **Subnet Mask**, and **Default Gateway** of the Switch. If you enable BOOTP, you do not need to configure any IP parameters because a BOOTP server automatically assigns IP configuration parameters to the Switch. If you enable DHCP, a Dynamic Host Configuration Protocol request will be sent when the Switch is powered up. Once you have selected a setting under **Get IP From**, click **Apply** to activate the new settings.

The information is described as follows:

MAC Address – The Ethernet address for the device. Also known as the physical address

Get IP From – There are three choices for how the Switch receives its IP Address settings: *Manual*, *BOOTP*, and *DHCP*.

IP Address – The host address for the device on the TCP/IP network.

Subnet Mask – The address mask that controls subnetting on your TCP/IP network.

Default Gateway – The IP address of the device—usually a router—that handles connections to other subnets and/or other TCP/IP networks.

VID – The VLAN ID number.

Switch Information

Switch Information Basic Setting	
Device Type	D-Link DES-3226 Ethernet Switch
External Module Type	None
MAC Address	00:10:27:32:26:b1
Boot PROM Version	1.00.003
Firmware Version	6.00.111
Base Module Version	2B1
External Module Version	
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Apply	

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

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

The information is described as follows:

Device Type – A description of the Switch type.

MAC Address – The Ethernet address for the device.

Boot PROM Version – Version number for the firmware chip. This information is needed for new runtime software downloads.

Firmware Version – Version number of the firmware installed on the Switch. This can be updated by using the **Update Firmware** window in the **Reset and Update** section.

Base Module Version – Version number of the base module.

System Name – A user-assigned name for the Switch.

System Location – A user-assigned description for the physical location of the Switch.

System Contact – Name of the person to contact should there be any problems or questions with the system. You may also want to include a phone number or extension.

Advanced Settings

Switch Information Advanced Settings	
Auto Logout	10 Minutes
MAC Address Aging Time	300
IGMP Snooping	Disabled
GVRP Status	Disabled
Telnet Status	Enabled
Web Status	Enabled
Group Address Filter Mode	Forward All Unregister
Scheduling Mechanism for CoS Queues	Strict
Trunk Load Sharing Algorithm	Source Addr
Switch GMRP	Disabled
Switch 802.1X	Disabled
Switch Filtering EAPOL PDU	Yes
Traffic Segmentation	Enabled
Secure Shell	Enabled

Apply

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

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

The information in the window is described as follows:

Auto-Logout [10 Minutes]– This sets the time the interface can be idle before the Switch automatically logs-out the user. The options are 2 minutes, 5 minutes, 10 minutes, 15 minutes, or Never.

MAC Address Aging Time [300] – This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between 10 and 1,000,000 seconds.

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

IGMP Snooping [Disabled] – This setting enables Internet Group Management Protocol (IGMP) Snooping, which enables the Switch to read IGMP packets being forwarded through the Switch in order to obtain forwarding information from them (learn which ports contain Multicast members).

GVRP Status [Disabled] – Group VLAN Registration Protocol is a protocol that allows members to dynamically join VLANs. This is used to enable or disable GVRP on the Switch

Telnet Status [Enabled] – Toggle to *Enabled* to allow access to the Switch over the network using the TCP/IP Telnet protocol.

Web Status [Enabled] – You can also use a Web-based browser to manage the Switch by toggling to *Enabled*.

Group Address Filter Mode [Forward All Unregister] – The IGMP filter mode for processing multicast packets. The options are *Forward All*, *Forward All Unregister*, and *Filtered All Unregister*.

Scheduling Mechanism for CoS Queues [*Strict*] – There are two Class of Service queue options, *RoundRobin* and *Strict*. If *Strict* is selected, when the highest priority queue is full, those packets will be the first to be forwarded. If *RoundRobin* is selected, the forwarding is based on the settings made on the **Class of Service Configuration** screen.

Trunk Load Sharing Algorithm [*Source Addr*] – The trunk load sharing options are *Dst Address*, *Src&Dst Address*, and *Src Address*.

Switch GMRP [*Disabled*] – This allows you to set Group Multicast Registration Protocol (GMRP) for the whole Switch.

Switch 802.1X [*Disabled*] – This allows you to set 802.1X for the whole Switch. The user may toggle between *Disabled*, *Port-Based* and *MAC-Based*.

Switch Filtering EAPOL PDU [*Yes*] – This option is only available if 802.1X is disabled. When enabled (*Yes*), this feature will allow the switch to filter Extensible Authentication Protocol Over LANs Packet Data Units (EAPOL PDU).

Traffic Segmentation [*Disabled*] – When this feature is *Enabled*, ports on the Switch are not able to communicate with one another except server port(s). If there is not an optional module present, Port 1 becomes the server port. If there is a 1-port optional module, this port will be the server port. If there is a 2-port optional module, both ports act as server ports.

Secure Shell [*Enabled*] – When this feature is *Enabled*, the switch encrypts all transmitted data for secure remote access over IP networks.

Port Configuration

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

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

Figure 7-4. Port Configuration window

Select the port you want to configure by using the drop-down menus in the **From** and **To** fields or click on the port in the Switch front panel display at the top of the window. Follow these steps:

Enable or disable the port. If you choose *Disabled* in the **State** field, devices connected to that port cannot use the Switch, and the Switch purges their addresses from its address table after the MAC address aging time elapses.

Configure the **Speed/Duplex** setting for the port. Select *Auto* to allow the port to select the best transmission speed, duplex mode and flow control settings based on the capabilities of the device at the other end. The other selections allow you to force

the port to operate in the specified manner. Select *100M/FULL* for port operation at 100 Mbps and full duplex. Select *100M/HALF* for port operation at 100 Mbps and half duplex. Select *10M/FULL* for port operation at 10 Mbps and full duplex. Select *10M/HALF* for port operation at 10 Mbps and half duplex.

Configure the **Flow Control** field to disable or enable flow control for a specific port. 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.

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

Port Mirroring

Setup Port Mirroring																								
Source Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ingress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Both	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Target Port	Port 2																							
Status	Disabled																							
Apply																								
<p>Note(1): The "Source Port" and "Target Port" should be different, or the setup will be invalid.</p> <p>Note(2): The target port should be a non-trunked port.</p> <p>The Trunking Ports: None</p>																								

Figure 7-5. Port Mirroring window

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

To configure a mirror port, first select the **Source Port** from where you want to copy frames and the **Target Port**, which receives the copies from the source port. This is the port where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe. Next, select the **Source Direction**, *Ingress*, *Egress*, or *Both*, and change the *Status* pull-down menu to *Enabled*. Finally, click **Apply** to let the changes take effect.

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

Port LACP Trunking

Port LACP Trunking Settings

Group ID	<input type="text" value="1"/>																																																
Group Name	<input type="text"/>																																																
Type	<input type="text" value="TRUNK"/>																																																
State	<input type="text" value="Disabled"/>																																																
Member Ports	<table style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td style="width: 15px;">1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td> </tr> <tr> <td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24																										
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																										

Port LACP Trunking Table

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

Note: It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.

Figure 7-6. Port LACP Trunking Settings window

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

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

The Switch allows the creation of up to 6 port trunking groups, each group consisting of up to 8 links (ports). The trunked ports can be non-continuous (that is, have non-sequential port numbers). All of the ports in the group must be members of the same VLAN. Further, the trunked ports must all be of the same speed and should be configured as full duplex.

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

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

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

The Link Aggregate Control Protocol (LACP) allows you to bundle several physical ports together to form one logical port. After the negotiation of LACP, these candidates of trunking ports could be trunked as a logical port. If any one of the

connected ports pair has no LACP capability, these two ports will stand as regular ports until the success of LACP communication. Same as traditional port trunking as explained above, the member ports of a LACP trunk group only can be formed a trunk with a peer LACP trunk group.

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

Group ID [1] – This field is for a group ID number for the port trunking group.

Group Name [] – Enter a name for the port trunking group.

Type [TRUNK] – If *LACP* is selected, each member of the port trunking group must support the Link Aggregate Control Protocol. There is no protocol requirement if *TRUNK* is selected.

State [Disabled] – This field can be toggled between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.

Member ports – Check each port of the port trunking group.

IGMP Snooping

VLAN ID	State	Querier State	Robustness Variable	QueryInterval	MaxResponse	Add/Modify
1	Enabled	Non-Querier	2	125	10	Apply

VID	VLAN Name	State	Age Out	Querier State	Delete
1	DEFAULT_VLAN	Enabled	260	Non-Querier	X

Figure 7-7. IGMP Snooping Settings window

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

To set up IGMP snooping, enter a VLAN ID number in the first field and change the **State** field to *Enabled*. Next, select the desired setting in the **Querier State** field—this determines the version of IGMP that is used in your network—and enter values in the following three fields. A value between 1 and 255 can be entered for the **Robustness Variable** (default is 2). The **Query Interval** can be set between 1 and 65535 seconds. This sets the time between IGMP queries. The **Max Response** allows a setting between 1 and 25 seconds and specifies the maximum amount of time allowed before sending a response report. Click **Apply** to make the settings effective.

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

VLAN ID [1] – Enter a VLAN ID number in this field.

State [Enabled] – Use the drop-down menu to enable or disable IGMP settings.

Querier State [Non-Querier] – Select from *Non-Querier*, *V1-Querier*, and *V2-Querier*. This is used to specify the IGMP version (1 or 2) that will be used by the IGMP interface when making queries.

Robustness Variable [2] – A tuning variable to allow for sub-networks that are expected to lose a large number of packets. A value between 1 and 255 can be entered, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.

Query Interval [125] – Allows the entry of a value between 1 and 65535 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.

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

Add/Modify – Click this hyperlink to add or modify an IGMP entry on this window.

Delete – Click this hyperlink to delete an IGMP entry on this window.

Port GMRP

Port GMRP Settings			
From	To	GMRP State	Apply
Port 1 ▾	Port 1 ▾	Off ▾	Apply

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

Figure 7-8. Port GMRP Settings window

This window allows you to turn on or turn off Group Multicast Registration Protocol (GMRP) on specified ports. Click **Apply** to let your changes take effect.

Diffserv Settings

Port Diffserv Settings					
From	To	Diffserv	Mode	Value	Apply
Port 1	Port 1	Disabled	Force Overwrite	0	Apply

Port Diffserv Table			
Port	Diffserv	Mode	Value
1	Disabled		
2	Disabled		
3	Disabled		
4	Disabled		
5	Disabled		
6	Disabled		
7	Disabled		
8	Disabled		
9	Disabled		
10	Disabled		
11	Disabled		
12	Disabled		
13	Disabled		
14	Disabled		
15	Disabled		
16	Disabled		
17	Disabled		
18	Disabled		
19	Disabled		
20	Disabled		
21	Disabled		
22	Disabled		
23	Disabled		
24	Disabled		

Figure 7-9. Port Diffserv Settings window

Differentiated Services brings scalable Quality of Service to the Internet Protocol environment, using a Type of Service (TOS) field in the IP header. The Switch has the capability to change the TOS precedence field (the first 3 bits of the TOS field) based on the packet classification.

This window allows you to set the following features:

From and **To** – Enter the port or ports to be set.

Diffserv [*Disabled*]– Choose from three options: *Disabled*, *DSCP*, and *TOS*.

Mode – Under *DSCP* (Differentiated Service Code Point), there are two choices, *Change if 0* or *Force Overwrite*. If *Force Overwrite* is selected, the differentiated services field of an incoming Ipv4 packet will be overwritten with the entered value. When *Change if 0* is selected, the differentiated services field of an incoming Ipv4 packet will be overwritten with the entered value if the original value of the DSCP field is zero. There are three choices under *TOS* (Type of Service): *TOS Overwrite 802.1p*, *802.1p Overwrite TOS*, and *Force Overwrite*. If *Force Overwrite* is selected, the IP TOS precedence of incoming Ipv4 packets will be overwritten with the entered value. If *TOS Overwrite 802.1p* is selected, the 802.1p tag control priority field of incoming Ipv4 packets will change to the value in the IP TOS precedence field. This action both alerts this field in the packet and changes the 802.1p priority used to determine the hardware CoS queue. If *802.1p Overwrite TOS* is selected, the IP TOS precedence of incoming Ipv4 packets will be changed to the value in the 802.1p tag control priority field.

Value – Enter either a DCSP or TOS value in this field.

Spanning Tree

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

STP Switch Settings

The Switch supports 802.1w Spanning Tree Protocol, which allows you to create alternative paths (with multiple switches or other types of bridges) in your network. See the Spanning Tree Algorithm section of the “*Switch Management and Operating Concepts*” chapter for a detailed explanation.

Switch Spanning Tree Settings	
STP Status	Disabled ▾
MaxAge(6-40 Sec)	20
Hello Time(1-10 Sec)	2
Forward Delay(4-30 Sec)	15
Priority(0-61440)	32768
STP Version	StpCompatibility ▾
TX Hold Count(1-10)	3
Apply	

Figure 7-10. Switch Spanning Tree Settings window

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

Parameters that you can change are:

STP Status [*Disabled*] – This drop-down menu allows you to enable the STP Status setting.

Max Age (6-40 Sec) [20] – The Maximum Age can be from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root ridge, your Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Hello Time (1-10 Sec) [2] – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

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 (0-65535 Sec) [32768] – A Bridge Priority can be from 0 to 65535. Zero is equal to the highest Bridge Priority.

STP Version [**StpCompatibility**] – Choose RSTP or STP Compatibility (default). 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(1-10) [3] – This is the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. Default value = 3.

STP Port Settings

STP Port Settings

From	To	Status	Cost	Priority	Migration	Edge	P-P	Apply
Port 1	Port 1	Disabled	0	128	Yes	Yes	Yes	Apply

The STP Port Information

Port	STP Status	Cost	Priority	Edge	P-P	Role	Port State
1	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
2	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
3	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
4	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
5	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
6	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
7	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
8	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
9	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
10	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
11	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
12	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
13	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
14	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
15	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
16	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
17	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
18	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
19	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
20	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
21	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
22	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled
23	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	NonStp	Forwarding
24	Enabled	0 / 200000	128	Yes / Yes	Auto / Yes	-	Disabled

Figure 7-11. STP Port Settings window

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

The information on the window is described as follows:

From – Enter the first port to be configured.

To – Enter the last port to be configured.

Status [*Disabled*] – The Spanning Tree Protocol state for a selected port can either be *Enabled* or *Disabled*.

Cost (1~65535) [*19*] – A port cost can be set between *1* and *65535*. The lower the cost, the greater the probability the port will be chosen as the designated port (chosen to forward packets).

Priority (0~255) [*128*] – A port priority can be set between *0* and *255*. The lower the priority, the greater the probability the port will be chosen as the root port.

Migration [*Yes*] – 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.

Type [*Permanent*] – Select the filter type, *Permanent* or *DeleteOnReset*.

Port Map – Allows the selection of ports that will be members of the static multicast group, are forbidden from being members, and ports that have no restrictions from joining dynamically.

VLANs

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

Static VLAN Entry

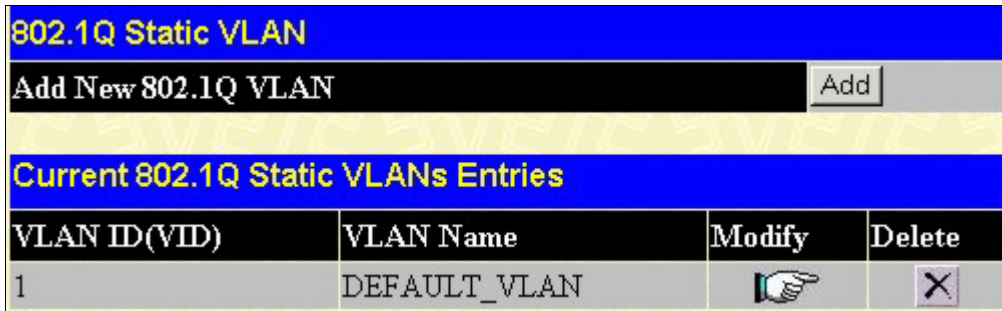


Figure 7-14. 802.1Q Static VLANs window

To add or modify an entry to this table, click the **Modify** icon and then fill in the appropriate information in the window below.

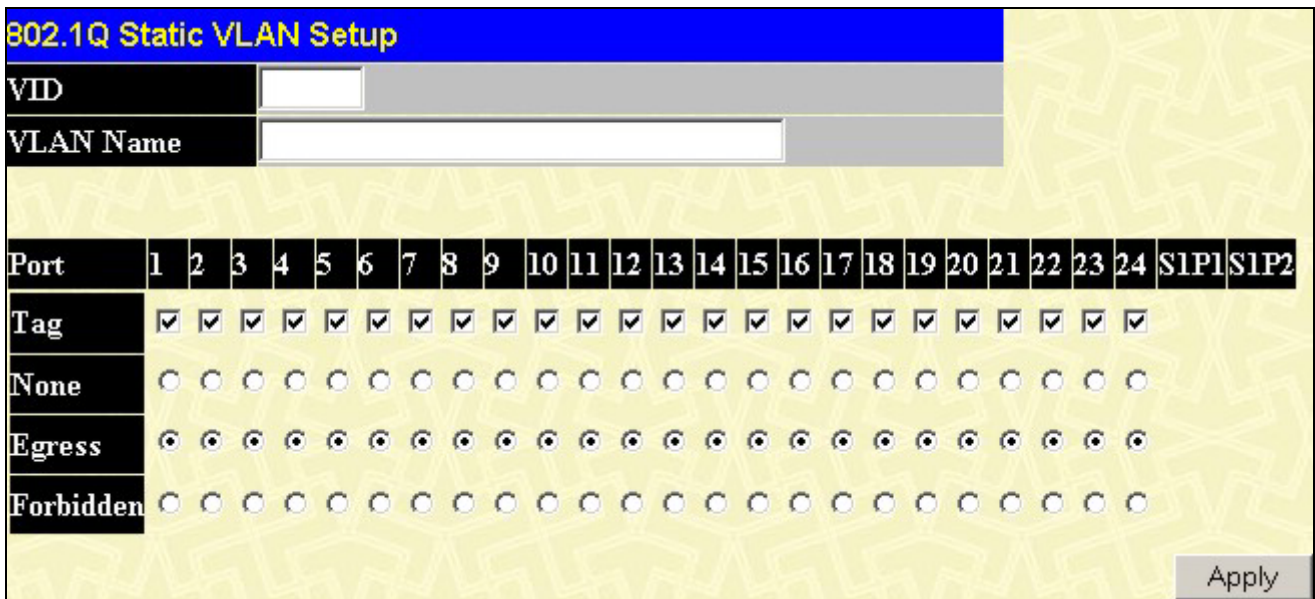


Figure 7-15. 802.1Q Static VLAN Setup window

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

The information on the window is described as follows:

VLAN ID (VID) – The VLAN ID of the VLAN that is being created.

VLAN Name [*DEFAULT_VLAN*] – The name of the VLAN that is being created.

Tag – Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.

None – Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.

Egress – Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.

Forbidden – Specifies the port that is not allowed to be a member of the VLAN.

Port VLAN ID (PVID)

802.1Q Port Settings					
From	To	PVID	Ingress	GVRP	Apply
Port 1	Port 1	1	Off	Off	Apply

8021Q Port Table			
Port	PVID	Ingress	GVRP
1	1	Off	On
2	1	Off	On
3	1	Off	On
4	1	Off	On
5	1	Off	On
6	1	Off	On
7	1	Off	On
8	1	Off	On
9	1	Off	On
10	1	Off	On
11	1	Off	On
12	1	Off	On
13	1	Off	On
14	1	Off	On
15	1	Off	On
16	1	Off	On
17	1	Off	On
18	1	Off	On
19	1	Off	On
20	1	Off	On
21	1	Off	On
22	1	Off	On
23	1	Off	On
24	1	Off	On

Figure 7-16. 802.1Q Port Settings window

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

Ingress filtering means that a receiving port will check to see if it is a member of the VLAN ID in the packet before forwarding the packet. GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the Switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports. Click **Apply** to let your changes take effect.

The information on the window is described as follows:

PVID [1] – The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet and ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.

Ingress [Off] – Specifies the port to check the VID of incoming packets against its VID or PVID. If the two are equal, the port will receive the packet. If the two are unequal, the port will drop the packet. This is used to limit traffic to a single VLAN.

GVRP [Off] – For each corresponding port, GARP VLAN Registration Protocol can be turned *On* or *Off*.

Port Bandwidth

The following four windows allow you to set and view ingress and egress bandwidth settings.

Ingress Bandwidth

Ingress Bandwidth Settings		
Port Num	Ingress Bandwidth(1-127 Units)	Add/Modify
Port 1	1	Apply

Ingress Bandwidth Setup Table				
Port	Units	KBytes	Port Speed	Delete
1	127	15875	100M/FULL	X
2	1	125	none	X

Figure 7-17. Ingress Bandwidth Settings window

To configure ingress bandwidth for a specific port, adjust the following fields and press APPLY.

Port Num: [1] – Choose which port (1-10) you would like to configure the Ingress Bandwidth for.

Ingress Bandwidth (1-127 Units) – Setting this field for a particular port will allow the user to limit the amount of packets the switch can receive. For an individual port, each unit is valued at 125 Kbytes per second. The maximum value setting for this field is 127.

Included in this screen is a table showing the Ingress Bandwidth settings currently implemented on the switch. The *Port Speed* value displays the current speed setting of a certain port. If there is no connection or link to a port, *none* will be displayed.

Egress Bandwidth

Egress Bandwidth Settings				
Port Num	Egress Bandwidth(1-127 Units)		Add/Modify	
Port 1	1		Apply	
Egress Bandwidth Setup Table				
Port	Units	KBytes	Port Speed	Delete
1	1	125	100M/FULL	X
7	127	15875	none	X

Figure 7-18. Egress Bandwidth Settings window

To configure the egress bandwidth for a specific port, adjust the following fields and press APPLY

Port Num: [1] – Choose which port you would like to configure the Egress Bandwidth for.

Egress Bandwidth (1-127 Units) – Setting this field for a particular port will allow the user to limit the amount of packets the switch can send to a node. For an individual port, each unit is valued at 125 Kbytes per second. The maximum value setting for this field is 127.

Included in this screen is a table showing the Egress Bandwidth settings currently implemented on the switch. The *Port Speed* value displays the current speed setting of a certain port. If there is no connection or link to a port, *none* will be displayed in the field.

Threshold of Broadcast

Threshold of Broadcast/Multicast/DA-Unknown Storm	
Monitoring Broadcast Storm	Disabled
Multicast Storm	Disabled
DA-Unknown Storm	Disabled
Threshold(Pkts/sec)	500
Apply	

Figure 7-19. Threshold of Broadcast/Multicast/DA-Unknown Storm window

The Switch allows you to set the threshold for three types of storms: broadcast, multicast, and destination address unknown. The higher the threshold, the more packets the Switch can accept per second. If the threshold is exceeded, any additional packets received will be dropped. Entering a low value means packets have a greater chance to exceed the threshold and, thus, be dropped from the Switch.

To use the features on this window, select *Enabled* from the drop-down menu, enter a threshold, and then click **Apply**.

Port Priority

Default Port Priority Assignment			
From	To	Priority(0-7)	Apply
Port 1 ▾	Port 1 ▾	0	Apply

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

Figure 7-20. Default Port Priority assignment window

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

Class of Traffic

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

Apply

Figure 7-21. Traffic Class Configuration window

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

Class of Service

Class of Service Configuration		
	Max. Packets(1-255)	Max. Latency(0-255)
Class-0	10	10
Class-1	10	10
Class-2	10	10
Class-3	10	10

Apply

Figure 7-22. Class of Service Configuration window

This window allows you to set the following features:

Max. Packets – The Class of Service scheduling algorithm starts from the highest CoS for a given port, sends the maximum number of packets, then moves on to the next lower CoS. The values that can be entered in this field are from 1 to 255. Entering zero instructs the Switch to continue processing packets until there are no more packets in the CoS transaction queue.

Max. Latency – The maximum allowable time a packet will stay in the CoS queue. The packets in this queue are not delayed more than the maximum allowable latency entered in this field. The timer is disabled when this field is set to zero. Each unit of this timer is equal to 16 microseconds. Max. Latency takes precedence over CoS scheduling algorithm.

Security Management

This section will help prepare the security features of the switch by describing how to configure the Port Security, Port Access Entity, Security IP, Security Shell and the Access Authentication Control screens, all of which can be found under the Security Management Menu along with various submenus.

Port Security

Port Security Settings					
From	To	Admin State	Max Addr(0-10)	Mode	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	1	DeleteOnReset ▾	Apply

Port Security Table			
Port	Admin State	Max. Learning Addr	Lock Address Mode
1	Disabled	1	DeleteOnReset
2	Disabled	1	DeleteOnReset
3	Disabled	1	DeleteOnReset
4	Disabled	1	DeleteOnReset
5	Disabled	1	DeleteOnReset
6	Disabled	1	DeleteOnReset
7	Disabled	1	DeleteOnReset
8	Disabled	1	DeleteOnReset
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset
13	Disabled	1	DeleteOnReset
14	Disabled	1	DeleteOnReset
15	Disabled	1	DeleteOnReset
16	Disabled	1	DeleteOnReset
17	Disabled	1	DeleteOnReset
18	Disabled	1	DeleteOnReset
19	Disabled	1	DeleteOnReset
20	Disabled	1	DeleteOnReset
21	Disabled	1	DeleteOnReset
22	Disabled	1	DeleteOnReset
23	Disabled	1	DeleteOnReset
24	Disabled	1	DeleteOnReset

Figure 7-23. Port Security Settings window

To set up security for a port or ports, enter the port or ports in the first two fields, change the **Admin State** to *Enabled*, enter the maximum number of addresses, the desired **Mode**, and then click **Apply**.

Security IP

This window is used to create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection. Enter the IP address(es) and click **Apply**.

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

Figure 7- 24. Security IP window

PAE Access Entity

The Port Access Entity section allows you to use the Switch's 802.1X port-based authentication feature.

Configure Authenticator

802.1X Authenticator Settings									
From	To	AdmDir	Port Control		Tx Period	Quiet Period			
Port 1	Port 1	both	forceUnauthorized		30	60			
Supp Timeout	Server Timeout	MaxReq	ReAuth Period		ReAuth	Apply			
30	30	2	3600		Enabled	Apply			

802.1X Authenticator Settings									
Port	AdmDir	Ctrl Stat	Tx Period	Quiet Period	Supp Timeout	Server Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	auto	30	60	30	30	2	3600	no
2	both	auto	30	60	30	30	2	3600	no
3	both	auto	30	60	30	30	2	3600	no
4	both	auto	30	60	30	30	2	3600	no
5	both	auto	30	60	30	30	2	3600	no
6	both	auto	30	60	30	30	2	3600	no
7	both	auto	30	60	30	30	2	3600	no
8	both	auto	30	60	30	30	2	3600	no
9	both	auto	30	60	30	30	2	3600	no
10	both	auto	30	60	30	30	2	3600	no
11	both	auto	30	60	30	30	2	3600	no
12	both	auto	30	60	30	30	2	3600	no
13	both	auto	30	60	30	30	2	3600	no
14	both	auto	30	60	30	30	2	3600	no
15	both	auto	30	60	30	30	2	3600	no
16	both	auto	30	60	30	30	2	3600	no
17	both	auto	30	60	30	30	2	3600	no
18	both	auto	30	60	30	30	2	3600	no
19	both	auto	30	60	30	30	2	3600	no
20	both	auto	30	60	30	30	2	3600	no
21	both	auto	30	60	30	30	2	3600	no
22	both	auto	30	60	30	30	2	3600	no
23	both	auto	30	60	30	30	2	3600	no
24	both	auto	30	60	30	30	2	3600	no

Figure 7-25. 802.1X Authenticator Settings window

This window allows you to set the following features:

From [] **To** [] – Enter the port or ports to be set.

AdmDir [both] – Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

PortControl [auto] – This allows you to control the port authorization state. Select *forceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *forceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. The third option is *auto*. This enables 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins

when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

TxPeriod [30] – This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period an EAP Request/Identity packet is transmitted to the client.

QuietPeriod [60] – This allows you to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.

SuppTimeout [30] – This value determines timeout conditions in the exchanges between the Authenticator and the client.

ServerTimeout [30] – This value determines timeout conditions in the exchanges between the Authenticator and the client.

MaxReq [2] – The maximum number of times that the switch will retransmit an EAP Request packet to the client before it times out the authentication session.

ReAuthPeriod [3600] – A constant that defines a nonzero number of seconds between periodic reauthentications of the client.

ReAuth [*Disabled*] – Determines whether regular reauthentication will take place on this port.

After configuring, click **Apply** to implement the settings.

PAE System Control

The PAE System control will help the user configure security settings for the ports of the switch. This section includes details on **Port Authenticating Settings**, **Initialize Ports** and **Reauthenticate Ports** windows.

Port Authenticating Settings

802.1X Capability Settings			
From	To	Capability	Apply
Port 1 ▾	Port 1 ▾	None ▾	Apply

802.1X Capability Table	
Port	Capability
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None
14	None
15	None
16	None
17	None
18	None
19	None
20	None
21	None
22	None
23	None
24	None

Figure 7-26. 802.1X Capability Settings window

To set up the Switch's 802.1X port-based authentication, select which ports are to be configured in the **From** and **To** fields. Next, enable the ports by selecting *Authenticator* from the drop-down menu under **Capability**. Click **Apply** to let your change take effect.

Initialize Ports(s)

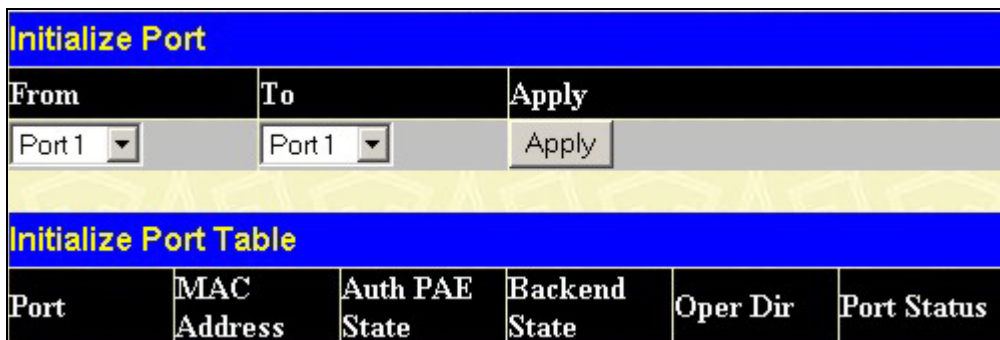


Figure 7-27. Initialize Port window

This window allows you to initialize a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s) once you have clicked **Apply**.

This window displays the following information:

Port – The port number.

AuthState – The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.*

BackendState – The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.*

AdmDir – The Administrative Controlled Directions are *both* and *in*.

OprDir – The Operational Controlled Directions are *both* and *in*.

PortStatus – The status of the controlled port can be *authorized, unauthorized, or N/A.*

Reauthenticate Ports(s)

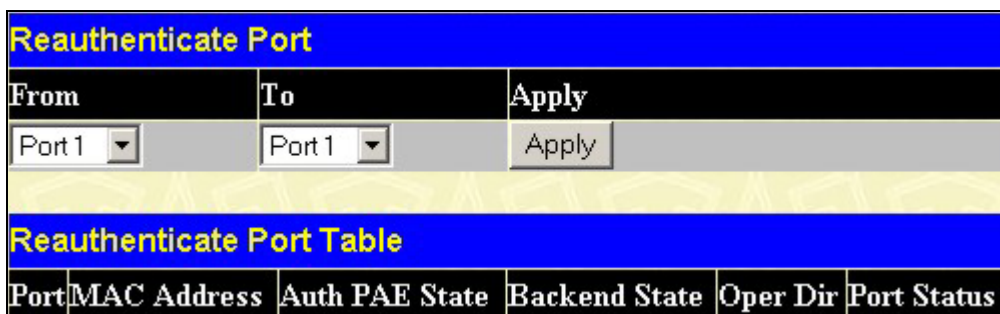


Figure 7-28. Reauthenticate Port window

This window allows you to reauthenticate a port or group of ports. The Reauthenticate Port Table displays the current status of the port(s) once you have clicked **Apply**.

This window displays the following information:

Port – The port number.

AuthState – The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.*

BackendState – The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.*

AdmDir – The Administrative Controlled Directions are *both* and *in*.

OprDir – The Operational Controlled Directions are *both* and *in*.

PortStatus – The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

Radius Server

The RADIUS feature of the switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker. The Web Manager offers three windows.

General Radius Server

General Radius Server Setting	
AuthProtocol	Radius Server
Radius Dead Time	1
Radius Time Out	10
Radius Maximum Retransmit	2
Accounting Method	Radius Server
Accounting Mode	Start and Stop

Figure 7-29. General Radius Server Setting window

This window allows you to set the following features:

AuthProtocol [*Radius Server*] – Toggle between the authentication protocol options: *Radius Server* (Support EAP) and *Local*.

Radius Dead Time [*1*] – This specifies the number of minutes a RADIUS server which is not responding to authentication requests is considered unavailable and is passed over by further requests for RADIUS authentication.

Radius Time Out [*10*] – This specifies the number of seconds NAS waits for a reply to a RADIUS request before transmitting the request.

Radius Maximum Retransmit [*2*] –This specifies the number of times NAS transmits each RADIUS request to the server before giving up.

Accounting Method [*Radius Server*] – To use a RADIUS Server, toggle from *None* to *Radius Server*.

Accounting Mode [*Start and Stop*] – Select the desired method: *Start and Stop*, *Stop only*, or *None*.

Authentic Radius Server

Authentic Radius Server Setting

Succession	First <input type="button" value="v"/>
Radius Server	<input type="text" value="0.0.0.0"/>
Authentic Port	<input type="text" value="1"/>
Accounting Port	<input type="text" value="1"/>
Key	<input type="text"/>
Confirm Key	<input type="text"/>
Accounting Method	Invalid <input type="button" value="v"/>

Current Radius Server(s) Settings Table

Succession	Radius Server	Auth UDP Port	Acct UDP Port	Valid State
First	0.0.0.0	0	0	Invalid
Second	0.0.0.0	0	0	Invalid
Third	0.0.0.0	0	0	Invalid

Figure 7-30. Authentic Radius Server Setting window

This window allows you to set the following features:

Succession [*First*] – Choose the desired RADIUS server to configure: *First*, *Second* or *Third*.

Radius Server [*0.0.0.0*] – Set the RADIUS server IP.

Authentic Port [*0*] – Set the RADIUS authentic server(s) UDP port. The default is *1813*.

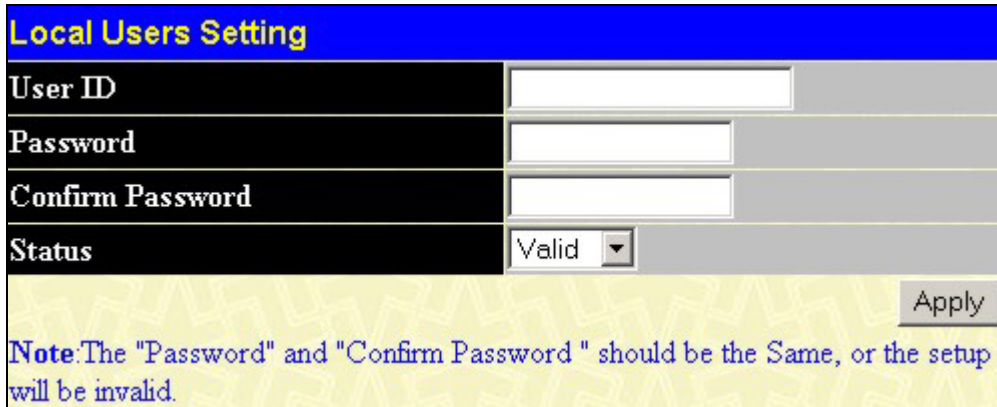
Accounting Port – Set the RADIUS account server(s) UDP port. The default is *1813*.

Key – Set the key the same as that of the RADIUS server.

Confirm Key – Confirm the shared key is the same as that of the RADIUS server.

Accounting Method [*Invalid*] – This allows you to set the RADIUS server as *Valid* or *Invalid*.

Local Users



Local Users Setting	
User ID	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Status	Valid ▾
Apply	
<p>Note: The "Password" and "Confirm Password " should be the Same, or the setup will be invalid.</p>	

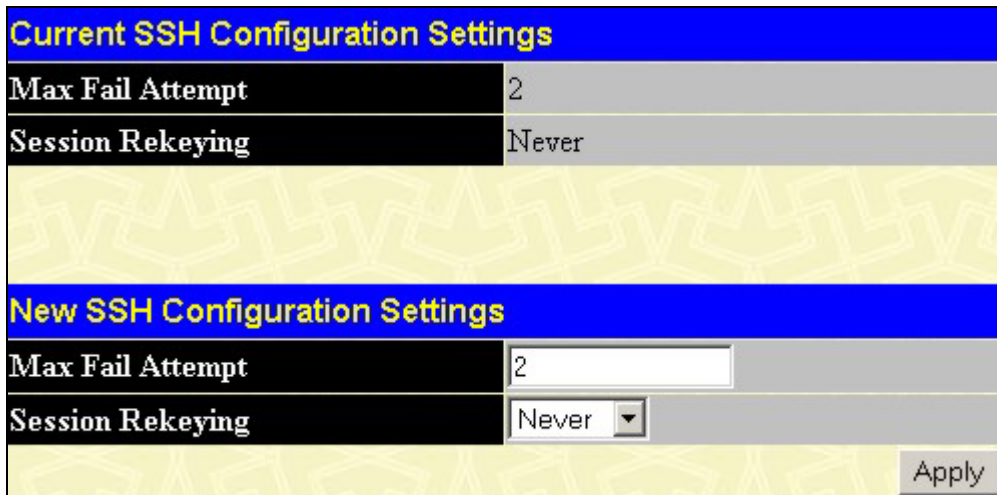
Figure 7-30. Local Users Setting window

The fields on this window allow you to add or remove local users.

Secure Shell

Secure Shell (SSH) is a mechanism for allowing secure remote access to management functions on a device. SSH provides a function similar to Telnet. Users can log into and configure the device using a publicly or commercially available SSH client program, just as they can with Telnet. However, unlike Telnet, which provides no security, SSH provides a secure, encrypted connection to the device. This section includes SSH Settings and SSH Algorithm windows.

SSH Settings



Current SSH Configuration Settings	
Max Fail Attempt	2
Session Rekeying	Never
New SSH Configuration Settings	
Max Fail Attempt	<input type="text" value="2"/>
Session Rekeying	Never ▾
Apply	

Figure 7- 31. SSH Settings window

This screen shows the current **Secure Shell** settings and allows the user to alter them, under the *New SSH Configurations Settings* header. The user may adjust:

Max Fail Attempt: [2] – Attempts may be set from 2 to 20 (default=2). Allows the user to set the number of times an outside guest may attempt to log on to the switch. With the **Max Fail Attempt** set at the default setting of 2, the outside guest must enter the appropriate settings in two attempts or that guest will have to start a new session.

Session Re-keying: [Never] – Sets the time period that the switch will change the security shell encryptions. Settings may be toggled to *Never, 10 min, 30 min, and 60 min.*

After making the adjustments, click **Apply** to implant them on the switch.

SSH Algorithm

This window allows the user to choose which encryption algorithms will be used on the switch's SSH security feature.

Encryption Algorithm	
3DES-cbc	Enabled ▾
Blow-fish-cbc	Enabled ▾
AES128-cbc	Enabled ▾
AES192-cbc	Enabled ▾
AES256-cbc	Enabled ▾
Arcfour	Enabled ▾
Cast128-cbc	Enabled ▾
Twofish128	Enabled ▾
Twofish192	Enabled ▾
Twofish256	Enabled ▾
Data Integrity Algorithm	
HMAC-SHA1	Enabled ▾
HMAC-MD5	Enabled ▾
Key Exchange Algorithm	
Diffie-Hellman	Enabled ▾
Authentication Algorithm	
Password	Enabled ▾
Publickey	Enabled ▾
Host based	Enabled ▾
Apply	

Figure 7- 32. SSH Algorithm window

The user may enable or disable:

Encryption Algorithm: When a client connects, it will select which algorithms to use from the list of algorithms specified by the user.

Data Integrity Algorithm: Choose the Data Integrity algorithm to apply to traffic on the switch. Your selection of a Data Integrity algorithm determines how IP packets are exchanged between the client and the server.

Key Exchange Algorithm: This algorithm allows two users to exchange a secret key over an insecure medium without any prior secrets.

Authentication Algorithm: These settings allow the user to choose the algorithms the client can access the switch with. The user may *Enable* or *Disable* Password, Publickey or Host-based encryptions.

After making the adjustments, click **Apply** to implant them on the switch.

Access Authentication Control

The Access Authentication Control feature provides a way to centrally validate users attempting to gain access to the switch using the Terminal Access Controller Access Control System (TACACS) protocol. TACACS is implemented in the switch's software to allow centralized control over access to servers.

Access Authentication Control Settings						
Authen. State	Disabled ▾					
Local Auth.	Enabled ▾					
Authentication Server Settings						
Succession	First ▾					
Authen. Protocol	TACACS ▾					
Authen. Server	0.0.0.0					
Authen. Port(1-65535)	49					
Server Time Out(1-255)	3					
Retry Count(1-9)	5					
Status	Invalid ▾					
						Apply
Current Access Authentication Table						
Succession	Server IP Addr	Protocol	Authen. Port	TimeOut	Retry	Status
First	0.0.0.0	TACACS	49	3	5	Invalid
Second	0.0.0.0	TACACS	49	3	5	Invalid
Third	0.0.0.0	TACACS	49	3	5	Invalid

Figure 7- 33. Access Authentication Control window

This window allows you to set the following features:

Auth. State: (Authentication State)<Disabled> – Use the pull down window to change the field to *Enabled* to implement the TACACS protocol. If the **Auth. State** is *Enabled*, the **Local Auth.** must be *Disabled*.

Local Auth: (Enabled) – This field must be toggled to *Disabled* for the TACACS protocol to be implemented. If *Enabled*, the switch will use the local authentication already implemented.

Succession: (First) – A total of three servers are supported for TACACS/TACACS+ authentication. Toggle between First, Second and Third to determine the order required by the user.

Authen. Server: [] – Enter the IP address of the server to be authenticated.

Authen. Protocol: <TACACS> – Toggle between TACACS, TACACS+ and XTACACS, depending on the security protocol desired.

Authen. Port: [49] – Edit the number in this field to change the port number from the default value of 49.

Server Time Out: [3] – Edit the value in the Server Time Out field to change how many seconds the device waits for a response from the TACACS server before either retrying the authentication request or determining that the TACACS server is unavailable and moving on to the next authentication method in the authentication-method list. The default is 3 seconds.

Retry Count: [5] – Edit the value in the Retry Count field to change how many times the device will resend an authentication request when the TACACS server does not respond.

Status: <Invalid> – Toggle to *Valid* to implement the server IP address with TACACS security enabled.

After making the adjustments, click **Apply** to implant them on the switch.

User Account Management

This section is used to create new user accounts for the switch and offers one window called User Accounts.

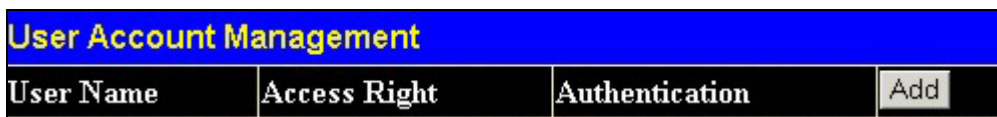


Figure 7- 34. User Account Management window

To add a new user, click **Add**:

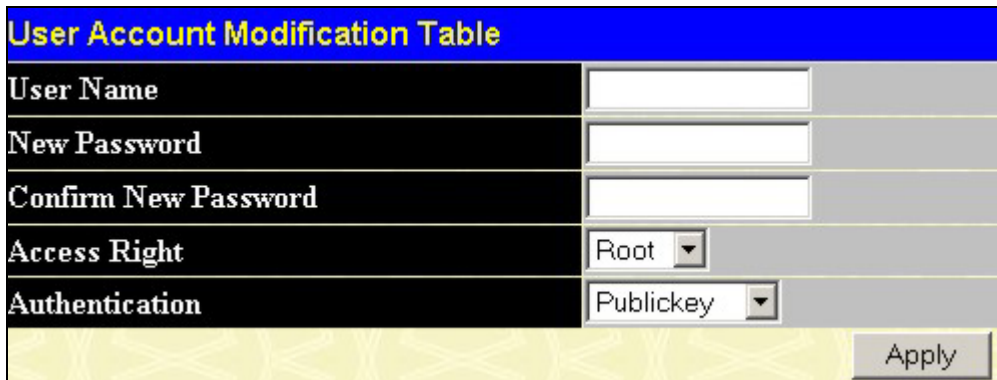


Figure 7- 35. User Account Modification Table

Modify the following fields and click **Apply**:

User Name: Type in the **Username** for the user account you wish to change.

New Password: If the password is to be changed, type in the new password you have chosen.

Confirm New Password: Type in the same new password in the following field to verify that you have not mistyped it.

Access Right: If the privilege level is to be changed, use the pull down menu to choose between *Root*, *User+* or *User*.

Authentication: Choose between *Publickey*, *Password*, and *Host-Based* to select the type of authentication that will be used by the new user.

SNMP Manager

The Simple Network Management Protocol is for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of the DES-3210/DES-3218/DES-3226. The user has a choice of SNMP v1&v2 or SNMP v1&v2&v3.

SNMP V1&V2

SNMP (V1/V2C) implements a rudimentary form of security by requiring that each request include a *community name*. If the Switch receives a request with a community name it does not recognize, it will trigger an authentication trap. The SNMP allows up to four different community names to be defined. You will need to coordinate these names with the community name settings you use in your network management system. In SNMP v1&v2 mode, Windows included in SNMP v1&v2 mode are SNMP Management Policy, SNMP Access Policy and SNMP Trap Receiver.

SNMP Management Policy

The SNMP Management Policy allows the user to change the SNMP version between V1&V2 and V1&V2&V3. Click **Apply** after the changes have been made.



Figure 7- 36. SNMP Management Policy window.

SNMP Community String Setup

This screen will allow the user to configure the *community string* on the switch for the SNMP security function.

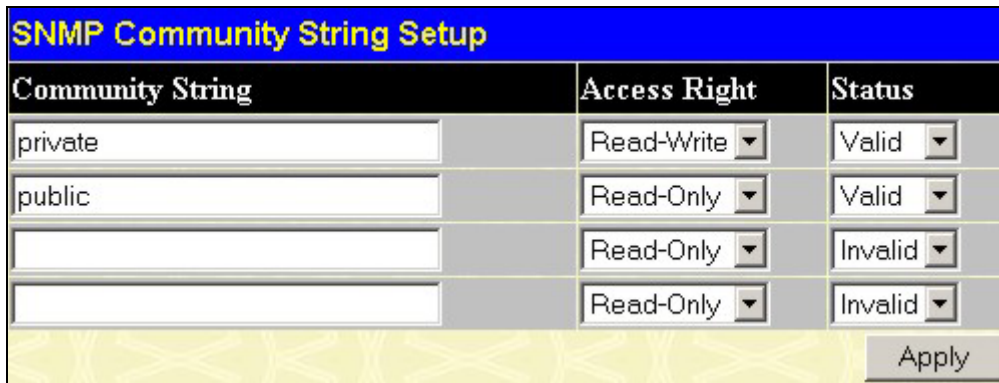


Figure 7- 37. SNMP Community String Setup window

The user may set the following fields:

SNMP Community String – The community string that will be included on SNMP packets sent to and from the switch. A station that is not configured for this community will not receive the packet.

Access Right – Allows each community to be separately set to either *Read Only*, meaning that the community member can only view switch settings or *Read/Write*, which allows the member to change settings in the switch.

Status – Determines whether this community name entry is *Valid* or *Invalid*. An entry can be disabled by changing its status to *Invalid*.

SNMP Trap Receiver

SNMP Trap Receiver Setup		
Trap Receiving Station	Community String	Status
0.0.0.0		Invalid ▾
0.0.0.0		Invalid ▾
0.0.0.0		Invalid ▾
0.0.0.0		Invalid ▾

Apply

Figure 7- 38. SNMP Trap Receiver Setup window

The user may set the following fields:

Trap Receiving Station – The IP address of the network management station to receive traps.

Community String – The community string that will be included on SNMP packets sent to and from the switch. A station that is not configured for this community will not receive the packet.

Status – Determines whether this community name entry is *Valid* or *Invalid*. An entry can be disabled by changing its status to *Invalid*.

SNMP V1&V2&V3

SNMP v.3 uses a more sophisticated authentication process that is separated into two parts. One part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions.

Windows included in SNMP V1&V2&V3 mode are SNMP Management Policy, Configure Community, Target Address, Target Parameter, Notify Table, Notify Filter Profile, Notify Filter, USM User, View VACM Context, VACM Group, VACM Access and VACM View Tree Family.

SNMP Management Policy

The SNMP Management Policy allows the user to change the SNMP version between V1&V2 and V1&V2&V3. If the user wishes to modify the Engine ID number, enter the ID into the **SNMP Engine ID** field. Click **Apply** after the changes have been made.

SNMP Management Policy	
SNMP Version	V1&V2&V3 ▾
SNMP Engine ID	800000ab030050803210c1

Apply

Figure 7- 39. SNMP Management Policy window

Configure Community

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. This window also shows the current community information implemented on the switch.

Community Table Setting					
Community Index	<input type="text"/>				
Community Name	<input type="text"/>				
C-Security Name	<input type="text"/>				
C-Context Name	<input type="text"/>				
Transport Tag	<input type="text"/>				
					Add/Modify
The Community Table Information					
Community Index	Community Name	C-Security Name	C-Context Name	Transport Tag	Delete
private	private	ReadWriteUser			X
public	public	ReadOnlyUser			X
					Total Number of Entries: 2

Figure 7- 40. Community Table Setting window

The user may configure the following fields:

Community Index: – Type a string of 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.

Community Name: – Type a string 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.

C-Security Name: – The user may enter two security names.

ReadOnly – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch

ReadWriteUser – 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.

C-Context Name: – This is the value originally determined for the notification.

Transport Tag: – Enter a value to use to select entries in the Target Address Table. Any entry in the Target Address Table that contains a tag value, which is equal to the value of the object selected. If this object is nil, no entries are selected.

Click **Apply** after the changes have been made.

Target Address

This window contains addresses of the targets for notifications in the SNMP function and information for establishing the transport parameters. This window also shows the current target address information implemented on the switch.

Target Address Settings																											
T-Address Name	Retry Count	Parameter Name			Transport Type																						
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>			UDP																						
Timeout	Notify Tag List	T-IP Address			Add/Modify																						
<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="button" value="Apply"/>																						
<table border="1"> <thead> <tr> <th colspan="7">The Target Address Information</th> </tr> <tr> <th>T-Address Name</th> <th>Retry Count</th> <th>Parameter Name</th> <th>Timeout</th> <th>Notify Tag List</th> <th>T-IP Address</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td colspan="7" style="text-align: right;">Total Number of Entries: 0</td> </tr> </tbody> </table>							The Target Address Information							T-Address Name	Retry Count	Parameter Name	Timeout	Notify Tag List	T-IP Address	Delete	Total Number of Entries: 0						
The Target Address Information																											
T-Address Name	Retry Count	Parameter Name	Timeout	Notify Tag List	T-IP Address	Delete																					
Total Number of Entries: 0																											

Figure 7-41. Target Address Settings window

The user may configure the following fields:

T-Address Name: Enter the name of the target address for notifications to be sent to.

Retry Count: Enter the number of retries to be attempted when a response is not received for a generated message. The default setting is 3.

Parameter Name: Enter a string to identify an entry in the SNMP Parameter Table. The identified entry contains SNMP parameters to be used when generated messages are sent to this transport address.

Transport Type: This field shows the system used to transport the notifications, which is UDP (User Datagram Protocol).

Timeout: Enter the time, in seconds, that the switch will wait for a response to an inform notification before resending that notification.

Notify Tag List: Enter the space-separated list of tag values to be used to select target addresses for a particular procedure.

T-IP Address: Enter the IP address that you would like to target.

Click **Apply** after the changes have been made.

Target Parameter

This window allows the user to manage target parameters used during notification generation to specify the communication parameters used for exchanges with notification recipients. This window also shows the current target parameter information implemented on the switch.

Target Params Settings					
T-Parameter Name	Msg Proc Model	T-Security Model	T-Security Level	T-Security Name	Add/Modify
	SNMPv1	SNMPv1	NoAuthNoPriv		Apply
The Target Params Information					
T-Parameter Name	Msg Proc Model	T-Security Model	T-Security Level	T-Security Name	Delete
Total Number of _Entries: 0					

Figure 7- 42. Target Params Settings window

The user may configure the following fields:

T-Parameter Name: – Enter a name to identify the parameter.

Msg Proc Mode: (SNMPv1) – Choose the message-processing model to be used when generating SNMP messages for this entry. The user may choose between SNMPv1, SNMPv2c and SNMPv3.

T-Security Model: (SNMPv1) – This field indicates the security model used to generate the message. The user may choose between *SNMPv1*, *SNMPv2* and *USM*. The SNMPv3 standard recommends the use of USM security model.

T-Security Level: <NoAuthNoPriv> – Choose the level of security to be used when generating SNMP messages, using this entry. This field may be toggled between noAuthNoPriv, authNoPriv and authPriv.

T-Security Name: Enter the principal on whose behalf SNMP messages are generated, using this entry.

Click **Apply** after the changes have been made.

Notify Table

The Notify Table contains groups of management targets to receive notifications and the type of notifications. The target addresses to receive notifications that are listed in target address table (see target group) are tagged here. This window also shows the current notify table information implemented on the switch.

Notify Table Settings			
Notify Name	Notify Type	Notify Tag	Add/Modify
	Trap		Apply
The Notify Table Information			
Notify Name	Notify Tag	Delete	
Total Number of _Entries: 0			

Figure 7- 43. Notify Table Settings window

The user may configure the following fields:

Notify Name: – Enter a name as a unique identifier used to index the Notify Table.

Notify Type: (Trap) – Type of notification to be used. On this switch, it is set at *Trap*, which cannot be altered.

Notify Tag: – Enter the textual ID used to identify notification targets in the SNMPv3 Target Table.

Click **Apply** after the changes have been made.

Notify Filter Profile

This table is used to associate a notification filter profile with a particular set of target parameters. This window also shows the current notify filter profile information implemented on the switch.

Notify Filter Profile Settings		
T-Parameter Name	NF-Profile Name	Add/Modify
<input type="text"/>	<input type="text"/>	Apply
Notify Filter Profile Information		
T-Parameter Name	NF-Profile Name	Delete
		Total Number of Entries: 0

Figure 7- 44. Notify Filter Profile Setup window

The user may configure the following fields:

T-Parameter Name: [] – Enter the name of the filter profile to be used when generating notifications using the corresponding entry in the Target Parameter Table.

NF-Profile Name: [] – Enter the name of the filter profile to be used when generating notifications using the corresponding entry in the Target Address Table.

Click **Apply** after the changes have been made.

Notify Filter

This is a table of filter profiles. Filter profiles are used to determine whether particular management targets should receive particular notifications. When a notification is generated, it must be compared with the filters associated with each management target that is configured to receive notifications. This window also shows the current notify filter information implemented on the switch.

Notify Filter Settings				
NF-Profile Name	Filter Mask	NF-Subtree OID	Filter Type	Add/Modify
<input type="text"/>	<input type="text"/>	<input type="text"/>	Included	Apply
The Notify Filter Information				
NF-Profile Name	Filter Mask	NF-Subtree OID	Filter Type	Delete
				Total Number of Entries: 0

Figure 7- 45. Notify Filter Settings window

The user may configure the following fields:

NF-Profile Name: – Enter the name of the filter profile to use when generating notifications using the corresponding entry in the **Target Address Table**. This entry must correspond to the identical entry in the previous screen.

Filter Mask: – Enter the name of the bit mask that, in combination with the corresponding instance of the Filter Subtree, defines a family of subtrees, which are included in or excluded from the filter profile.

NF-Subtree OID: – Enter a name indicating the MIB subtree which, when combined with the corresponding instance of the Filter Mask, defines a family of subtrees which are included in or excluded from the filter profile.

Filter Type: (Included) –Choose between *Include* and *Exclude* to indicate whether the family of filter subtrees defined by this entry are included in or excluded from a filter.

Click **Apply** after the changes have been made.

USM User

The USM Setting Table allows the administrator to define new user names and associated security information. You cannot modify existing mappings; you must delete and then recreate them with the correct information. This window also shows the current USM user information implemented on the switch.

USM User Setting			
User Name	<input type="text"/>		
Auth. Protocol	NONE ▾		
Auth. Password	<input type="text"/>		
Priv. Protocol	NONE ▾		
Priv. Password	<input type="text"/>		
			Add/Modify
USM User Information			
User Name	Auth. Protocol	Priv. Protocol	Delete
initial	NONE	NONE	X
Total Number of Entries: 1			

Figure 7- 46. USM User Setting window

The user may configure the following fields:

User Name: – Enter a name indicating the textual name of a user.

AuthProtocol: (NONE) – Choose between NONE, MD5 or SHA1 to choose the Authentication Protocol.

AuthPassword:– Enter the password used as part of the authentication process. The password is automatically manipulated to conform to the specific requirements of the specific authentication protocol. If no authentication protocol is selected, you do not need a password.

PrivProtocol: (NONE) – Toggle Between NONE and DES to choose the Privacy Protocol.

PrivPassword: [] – Enter the password used as part of the privacy process. The password is automatically manipulated to conform to the specific requirements of the specific privacy protocol. If no privacy protocol is selected, you do not need a password.

Click **Apply** after the changes have been made.

View VACM Context

View based Access Control Model (VACM) is a default access control model defined by SNMPV3 framework. The SNMPv3 agent has implemented the VACM MIB as a default access control model.

Here the user can enter a set of valid context names supported by the SNMPv3 agent. The received context name will be checked with this table in the access validation phase. Leaving the field empty (zero length) represents the default context.

This window also shows the current VACM context information implemented on the switch. Enter the **V-Context Name** and click **Apply**.

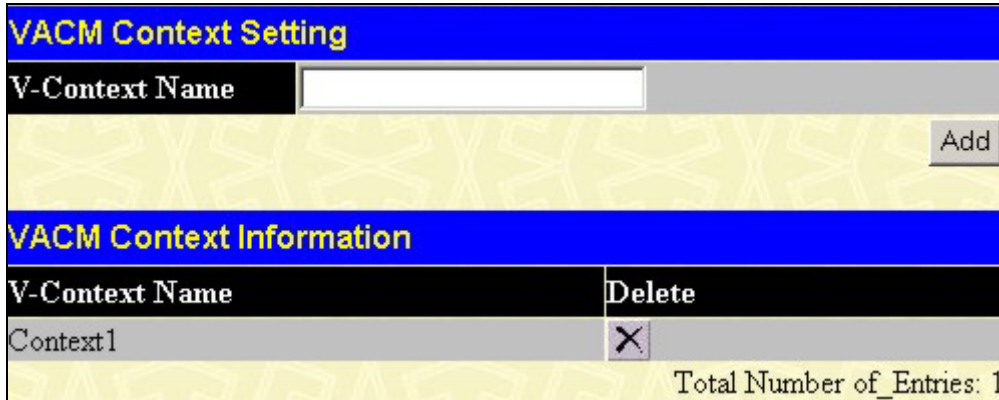


Figure 7- 47. VACM Context Setting window

VACM Group

This table maps a combination of security model and security name into a group name that is used to define an access control policy for a group of principals. This window also shows the current VACM group information implemented on the switch.

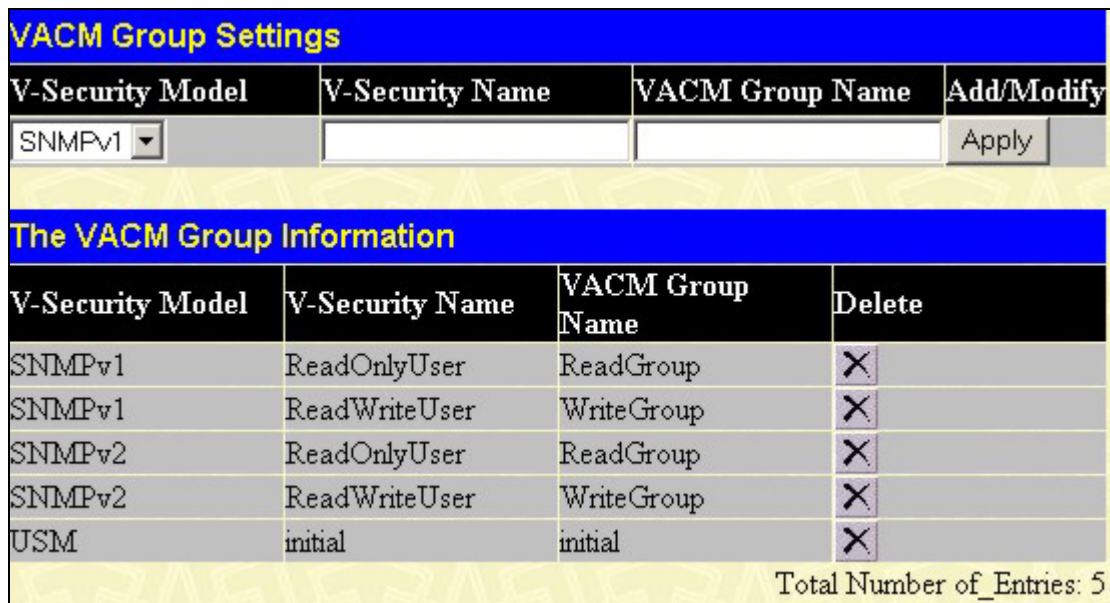


Figure 7- 48. VACM Group Settings window

The user may configure the following fields:

V-Security Model: (SNMPv1) – Choose between *USM*, *SNMPv1* or *SNMPv2c* to map the combination of a security model and security name into a group name.

V-Security Name: [] – Enter a security name for the principal, represented in a security model independent format, which is mapped by this entry to a group name.

VACM Group Name: [] – Enter the name of the group to which this entry (e.g., the combination of security model and security name) belongs. This group name is used as index into the VACM Access Table Setup to select an access control policy.

Click **Apply** after the changes have been made.

VACM Access

The VACM Access Table Setup is a table of access rights for groups. Each entry is indexed by a context prefix, a group name, a security model and a security level. To determine whether access is allowed, one entry from this table needs to be selected and the proper view name from that entry must be used for access control checking. This window also shows the current VACM access information implemented on the switch.

VACM Access Settings

VACM Group Name	V-Context Prefix	V-Security Model	V-Security Level
<input type="text"/>	<input type="text"/>	SNMPv1 ▾	NoAuthNoPriv ▾
Context Match	Read View Name	Write View Name	Notify View Name
Exact ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>

The VACM Access Settings Information

VACM Group Name	V-Context Prefix	V-Security Model	V-Security Level	Context Match	Read View Name	Write View Name	Notify View Name	Delete
initial		USM	NoAuthNoPriv	Exact	restricted		restricted	✕
ReadGroup		SNMPv1	NoAuthNoPriv	Exact	CommunityView		CommunityView	✕
ReadGroup		SNMPv2	NoAuthNoPriv	Exact	CommunityView		CommunityView	✕
WriteGroup		SNMPv1	NoAuthNoPriv	Exact	CommunityView	CommunityView	CommunityView	✕
WriteGroup		SNMPv2	NoAuthNoPriv	Exact	CommunityView	CommunityView	CommunityView	✕

Total Number of Entries: 5

Figure 7- 49. VACM Access Settings window

The user may configure the following fields:

VACM Group Name: – Enter the name of the group, which was entered in the same field in the previous screen.

V-Context Prefix:– In order to gain the access rights allowed by this conceptual row, a context name entered must match exactly (if the value of VACM Access Context Match is 'exact') or partially (if the value of VACM Access Context Match is 'prefix') to the value of the instance of this object.

V-Security Model: (SNMPv1) – Choose between USM, SNMPv1 or SNMPv2c order to gain the access rights allowed by this conceptual row.

V-Security Level: (noAuthNoPriv) – Choose between noAuthNoPriv, authNoPriv, or authPriv to enable the minimum level of security required in order to gain the access rights allowed by this conceptual row.

Context Match: (Exact) – Choose between *Exact* and *Prefix*. If the value of this object is exact, then all rows where the context name exactly matches VACM Access Context Prefix are selected. If the value of this object is prefix, then all rows where the context name whose starting octets exactly match VACM Access Context Prefix are selected. This allows for a simple form of wildcarding.

Read View Name: –Enter the value of this object that identifies the MIB view of the SNMP context to which this conceptual row authorizes read access.

Write View Name: – Enter the value of this object identifying the MIB view of the SNMP context to which this conceptual row authorizes write access.

Notify View Name: [] –Enter the value of this object identifying the MIB view of the SNMP context to which this conceptual row authorizes access for notifications.

Click **Apply** after the changes have been made.

VACM View Tree Family

This screen allows the user to alter the locally held information about families of subtrees within MIB views.

Each MIB view is defined by two sets of view subtrees:

- the included view subtrees, and
- the excluded view subtrees.

Every such view subtree, both the included and the excluded ones, is defined in this table.

This window also shows the current VACM view tree family information implemented on the switch.

VACM View Tree Family Settings

View Name	View Mask	Subtree OID	View Type	Add/Modify
			Included ▾	Apply

The VACM View Tree Family Information

View Name	View Mask	Subtree OID	View Type	
restricted		1.3.6.1.2.1.1	Included	✕
restricted		1.3.6.1.2.1.11	Included	✕
restricted		1.3.6.1.6.3.10.2.1	Included	✕
restricted		1.3.6.1.6.3.11.2.1	Included	✕
restricted		1.3.6.1.6.3.15.1.1	Included	✕
CommunityView		1	Included	✕
CommunityView		1.3.6.1.6.3	Excluded	✕
CommunityView		1.3.6.1.6.3.1	Included	✕

Total Number of Entries: 8

Figure 7- 50. VACM View Tree Family Settings window

The user may configure the following fields:

View Name: – Enter the name for a family of view subtrees.

View Mask: – Enter the bit mask, which, in combination with the corresponding VACM View Tree Family Subtree, defines a family of view subtrees.

Subtree OID: – Enter a name indicating the MIB subtree which when combined with the corresponding VACM View Tree Family Mask, defines a family of view subtrees.

View Type: (Included) –Choose between *Included* or *Excluded* to indicate whether the corresponding instances of VACM View Tree Family Subtree and VACM View Tree Family Mask define a family of view subtrees will be included in or excluded from the MIB view.

Click **Apply** after the changes have been made.

Monitoring

This category includes: Port Utilization, Packets (Received (RX), UMB_cast (RX), and Transmitted (TX)), Errors (Received (RX) and Transmitted (TX)), Size (Packet), MAC Address, IGMP Snooping, Dynamic Group Registration, VLAN Status, and Port Access Control, as well secondary screens.

Port Utilization

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

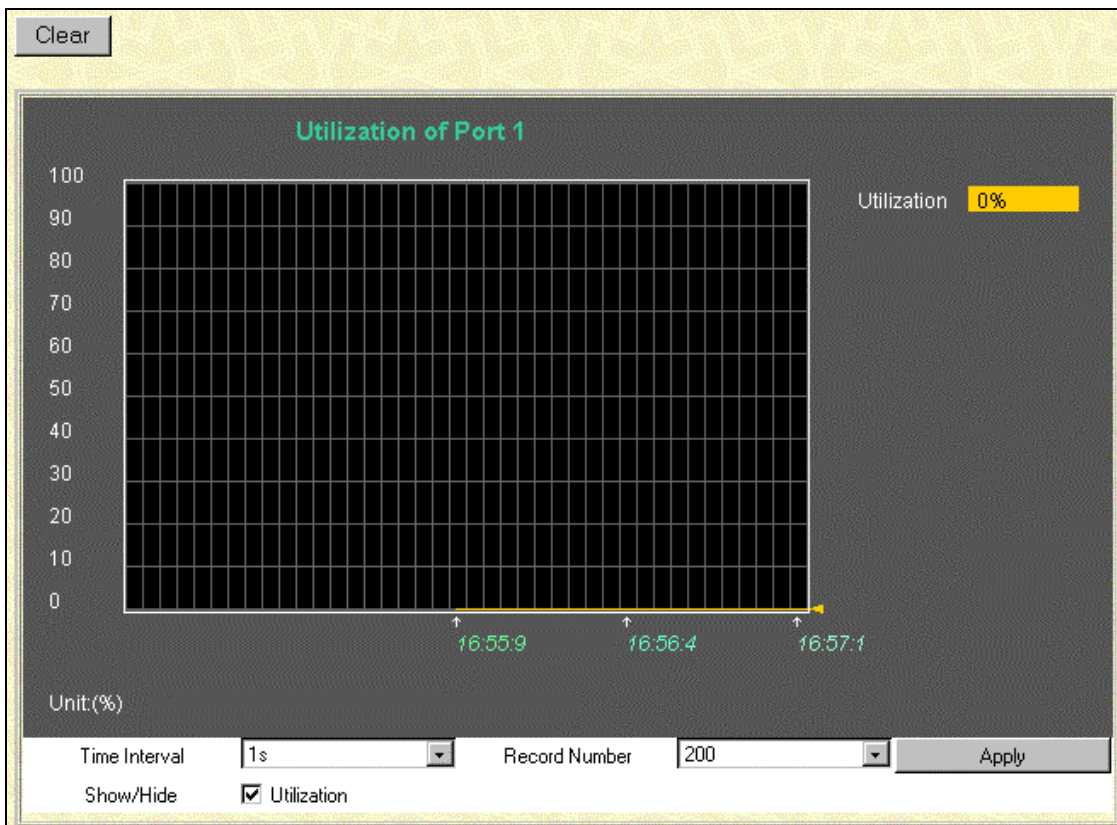


Figure 7-51. Utilization window

The information is described as follows:

Time Interval [1s] – Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.

Record Number [200] – Select number of times the Switch will be polled between 20 and 200. The default value is 20.

Show/Hide – Check whether or not to display Utilization.

Clear – Clicking this button clears all statistics counters on this window.

Packets

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

Received (RX)

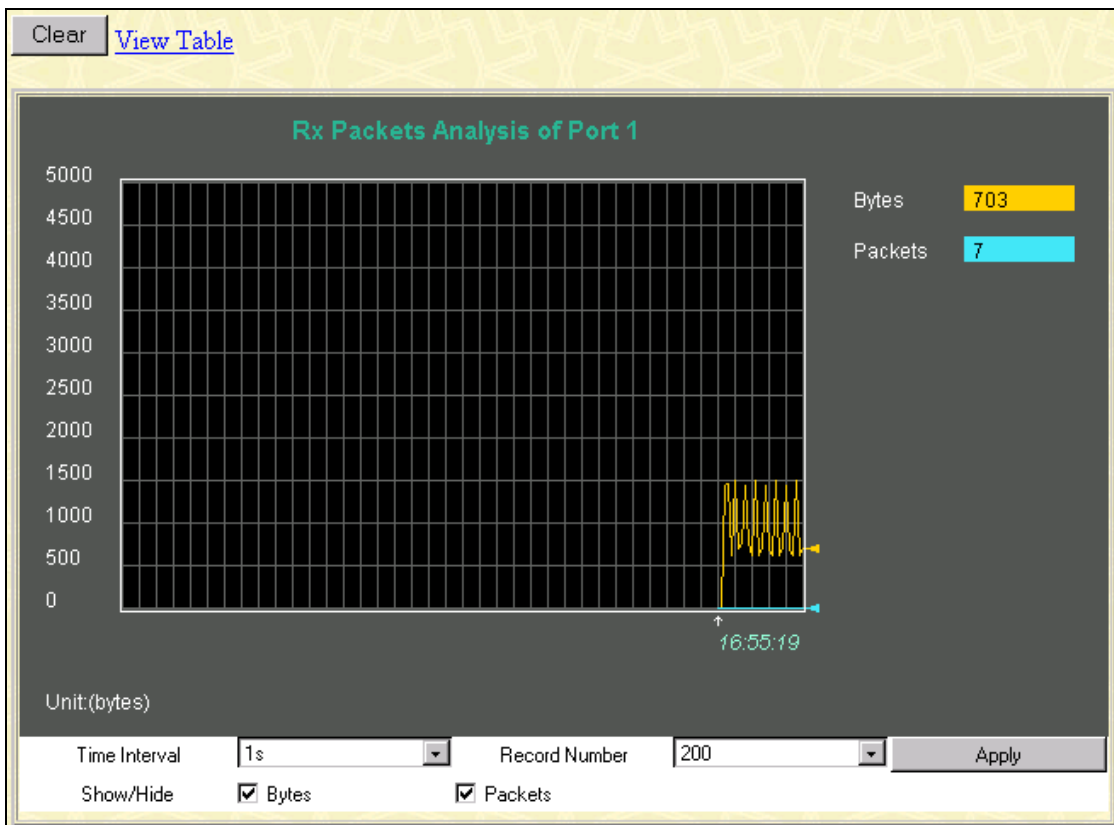


Figure 7-52. Rx Packets Analysis window (Line Chart)

[View Line Chart](#)

Packet Analysis of Port 1 Time Interval: 1s OK

Rx Packets	Current	Total	Average	Peak
Bytes	7395	253192985	7395	590237
Packets	36	2865417	36	7156

Rx Packets	Current	Total	Average	Peak
Unicast	9	2772985	9	7107
Multicast	1	11308	1	132
Broadcast	26	81124	26	268

Tx Packets	Current	Total	Average	Peak
Bytes	1014	2455554	1014	13859
Packets	7	7526	7	15

Figure 7-53. Rx Packets Analysis window (Table)

The information is described as follows:

Time Interval [1s] – Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.

Record Number [200] – Select number of times the Switch will be polled between 20 and 200. The default value is 20.

Bytes – Counts the number of bytes received on the port.

Packets – Counts the number of packets received on the port.

Multicast – Counts the total number of good packets that were received by a multicast address.

Broadcast – Counts the total number of good packets that were received by a broadcast address.

Show/Hide – Check whether or not to display Bytes and Packets.

Clear – Clicking this button clears all statistics counters on this window.

View Table – Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart – Clicking this button instructs the Switch to display a line graph rather than a table.

UMB-cast (RX)

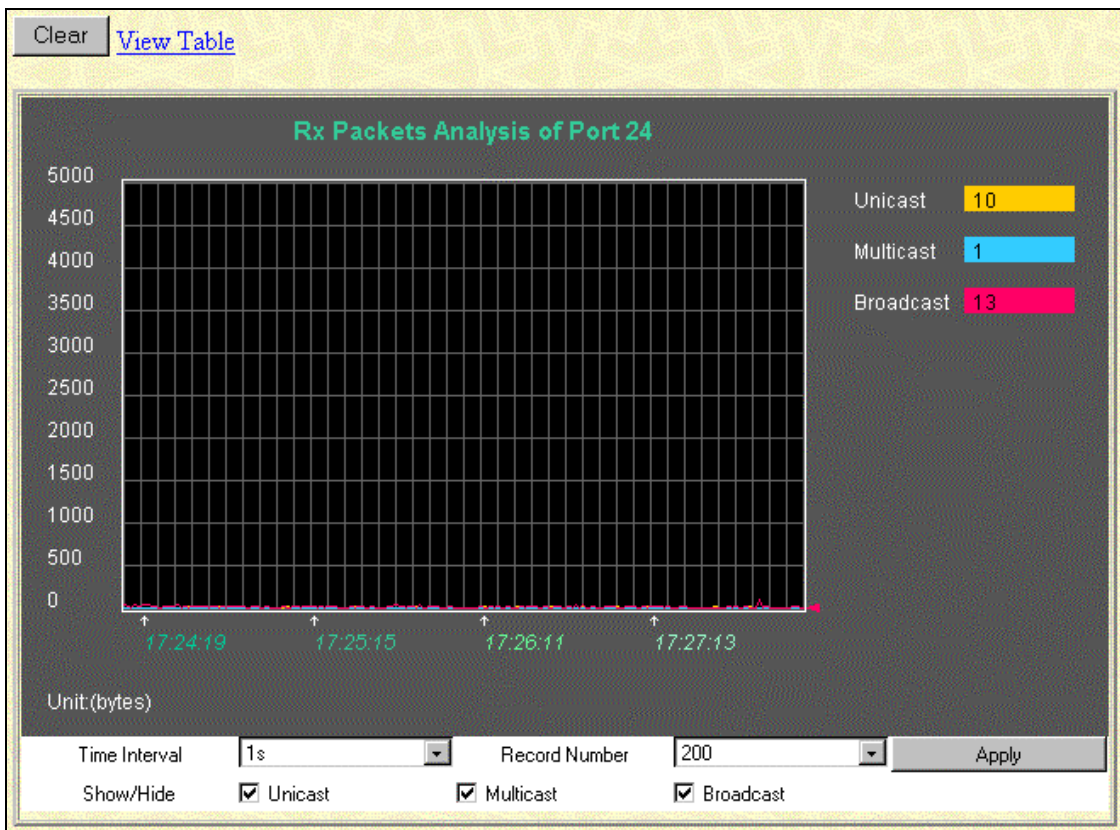


Figure 7-54. Rx Packets Analysis window for UMB (Line Chart)

[View LineChart](#)

Packet Analysis of Port 1 Time Interval

Rx Packets	Current	Total	Average	Peak
Bytes	6587	252165938	6587	590237
Packets	39	2860170	39	7156

Rx Packets	Current	Total	Average	Peak
Unicast	6	2772266	6	7107
Multicast	8	10682	8	132
Broadcast	25	77222	25	268

Tx Packets	Current	Total	Average	Peak
Bytes	661	2257619	661	13859
Packets	5	6882	5	15

Figure 7-55. Rx Packets Analysis window for MBU (Table)

The information is described as follows:

Time Interval [1s] – Select the desired setting between *1s* and *60s*, where “s” stands for seconds.

Record Number [200] – Select number of times the Switch will be polled between *20* and *200*.

Unicast – Counts the total number of good packets that were received by a unicast address.

Multicast – Counts the total number of good packets that were received by a multicast address.

Broadcast – Counts the total number of good packets that were received by a broadcast address.

Show/Hide – Check whether or not to display Multicast, Broadcast, and Unicast Packets.

Clear – Clicking this button clears all statistics counters on this window.

View Table – Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart – Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

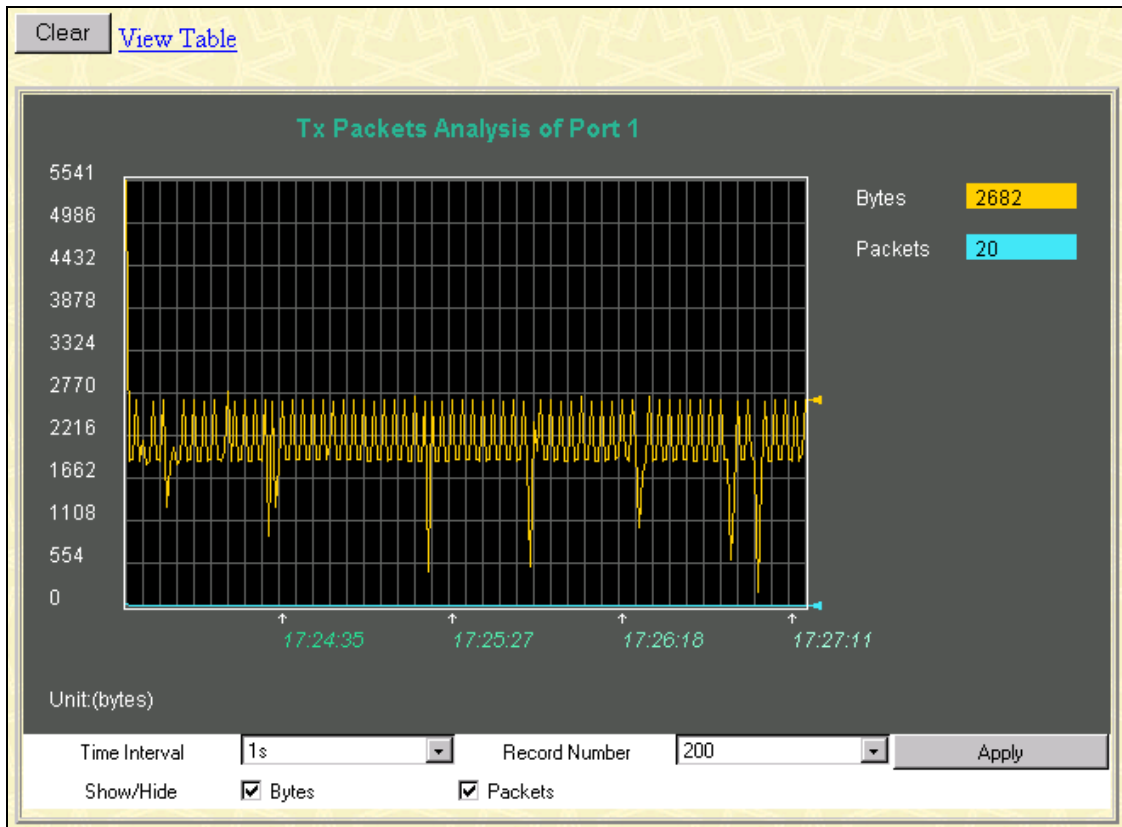


Figure 7-56. Tx Packets Analysis window (Line Chart)

[View LineChart](#)

Packet Analysis of Port 1 Time Interval: 1s OK

Rx Packets	Current	Total	Average	Peak
Bytes	6567	252165938	6567	590237
Packets	39	2860170	39	7156

Rx Packets	Current	Total	Average	Peak
Unicast	6	2772266	6	7107
Multicast	8	10882	8	132
Broadcast	25	77222	25	268

Tx Packets	Current	Total	Average	Peak
Bytes	661	2257619	661	13859
Packets	5	6882	5	15

Figure 7-57. Tx Packets Analysis window (Table)

The information is described as follows:

Time Interval [1s] – Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.

Record Number [200] – Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Bytes – Counts the number of bytes successfully sent from the port.

Multicast – Counts the total number of good packets that were received by a multicast address.

Broadcast – Counts the total number of good packets that were received by a broadcast address.

Packets – Counts the number of packets successfully sent on the port.

Show/Hide – Check whether or not to display Bytes and Packets.

Clear – Clicking this button clears all statistics counters on this window.

View Table – Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart – Clicking this button instructs the Switch to display a line graph rather than a table.

Errors

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

Received (RX)

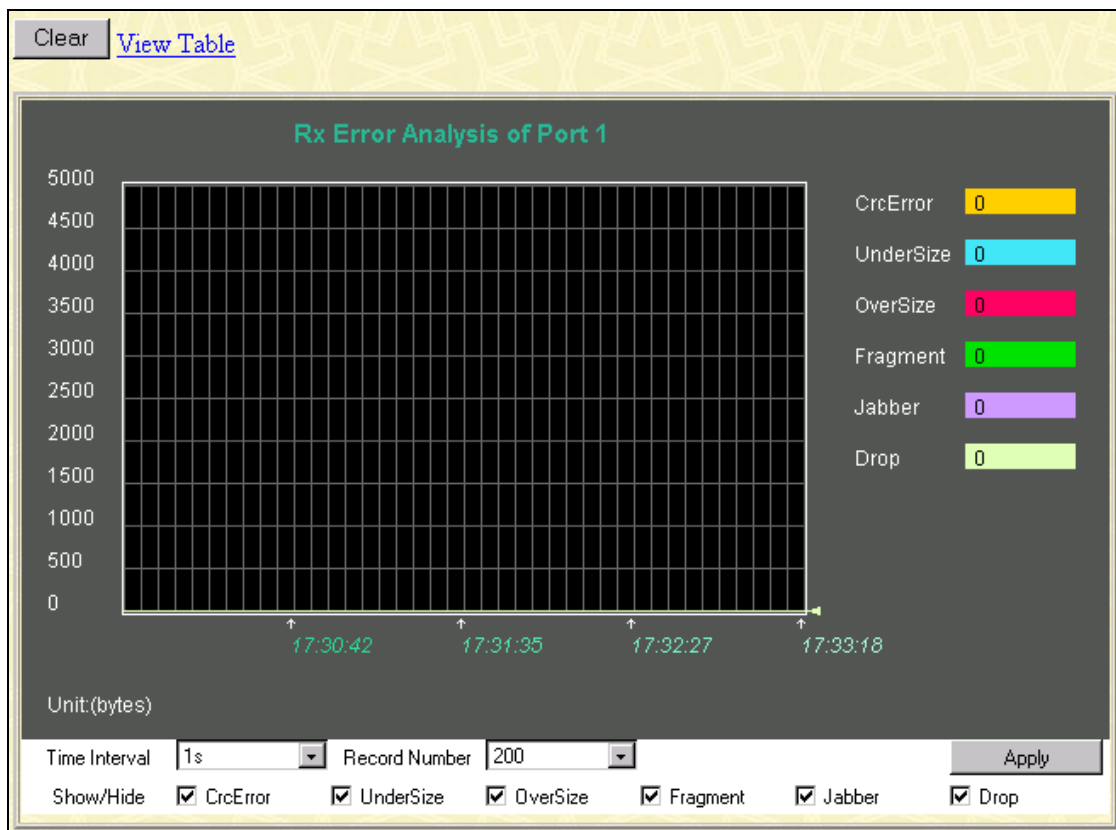


Figure 7-58. Rx Error Analysis window (Line Chart)

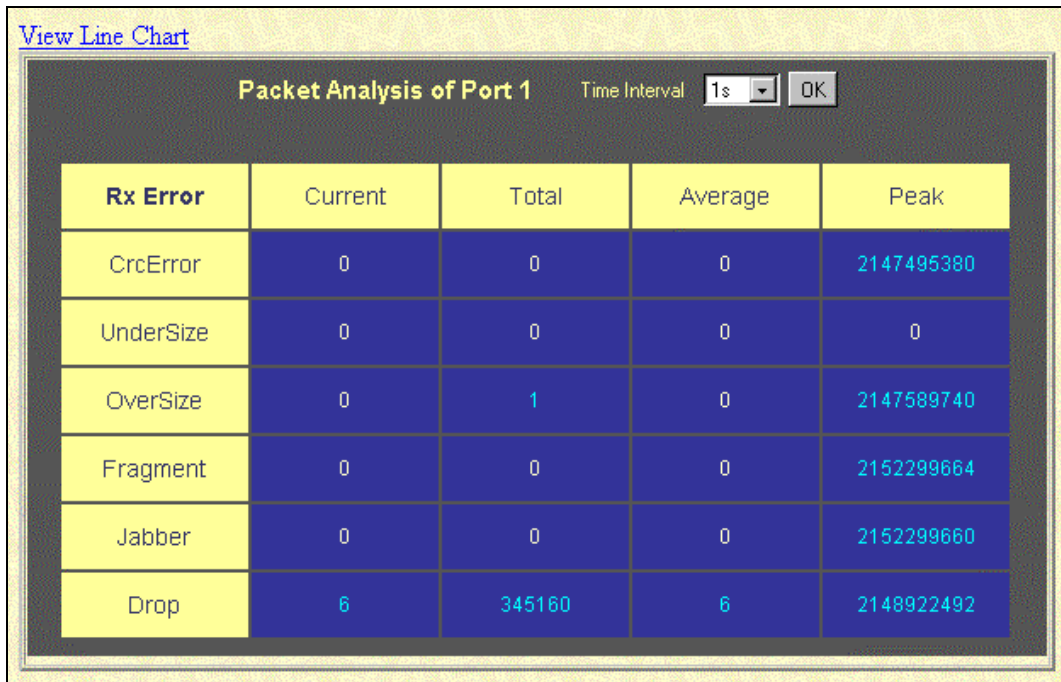


Figure 7-59. Rx Error Analysis window (Table)

The information is described as follows:

Time Interval [1s] – Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.

Record Number [200] – Select number of times the Switch will be polled between 20 and 200. The default value is 200.

CRCError – Counts otherwise valid frames that did not end on a byte (octet) boundary.

UnderSize – The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.

OverSize – Counts packets received that were longer than 1518 octets, or if a VLAN frame, 1522 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.

Fragment – The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

Jabber – The number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.

Drop – The number of frames, which are dropped by this port since the last Switch reboot.

Show/Hide – Check whether or not to display CrcError, UnderSize, OverSize, Fragment, Jabber, and Drop errors.

Clear – Clicking this button clears all statistics counters on this window.

View Table – Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart – Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

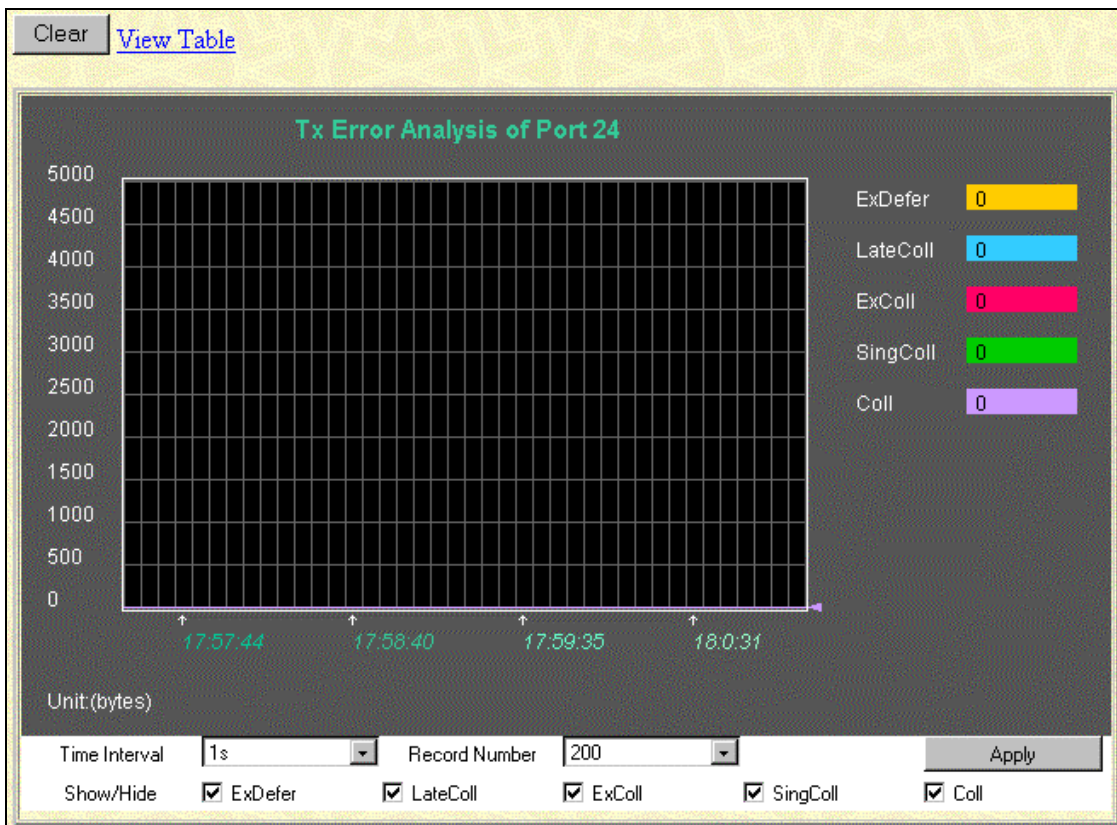


Figure 7-60. Tx Error Analysis window (Line Chart)

[View Line Chart](#)

Packet Analysis of Port 1 | Time Interval: 1s | OK

Tx Error	Current	Total	Average	Peak
ExDefer	0	0	0	2152299944
CrcError	4294987295	0	0	20
LateColl	0	0	0	2152520292
ExColl	0	0	0	1
SingColl	0	0	0	1
Coll	0	0	0	1

Figure 7-61. Tx Error Analysis window (Table)

The information is described as follows:

Time Interval [1s] – Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.

Record Number [200] – Select number of times the Switch will be polled between 20 and 200. The default value is 200.

ExDefer – Counts the number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.

CRCError – Counts otherwise valid frames that did not end on a byte (octet) boundary.

LateColl – Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Show/Hide – Check whether or not to display ExDefer, CrcError, and LateColl errors.

Clear – Clicking this button clears all statistics counters on this window.

View Table – Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart – Clicking this button instructs the Switch to display a line graph rather than a table.

Size

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

Packet Size

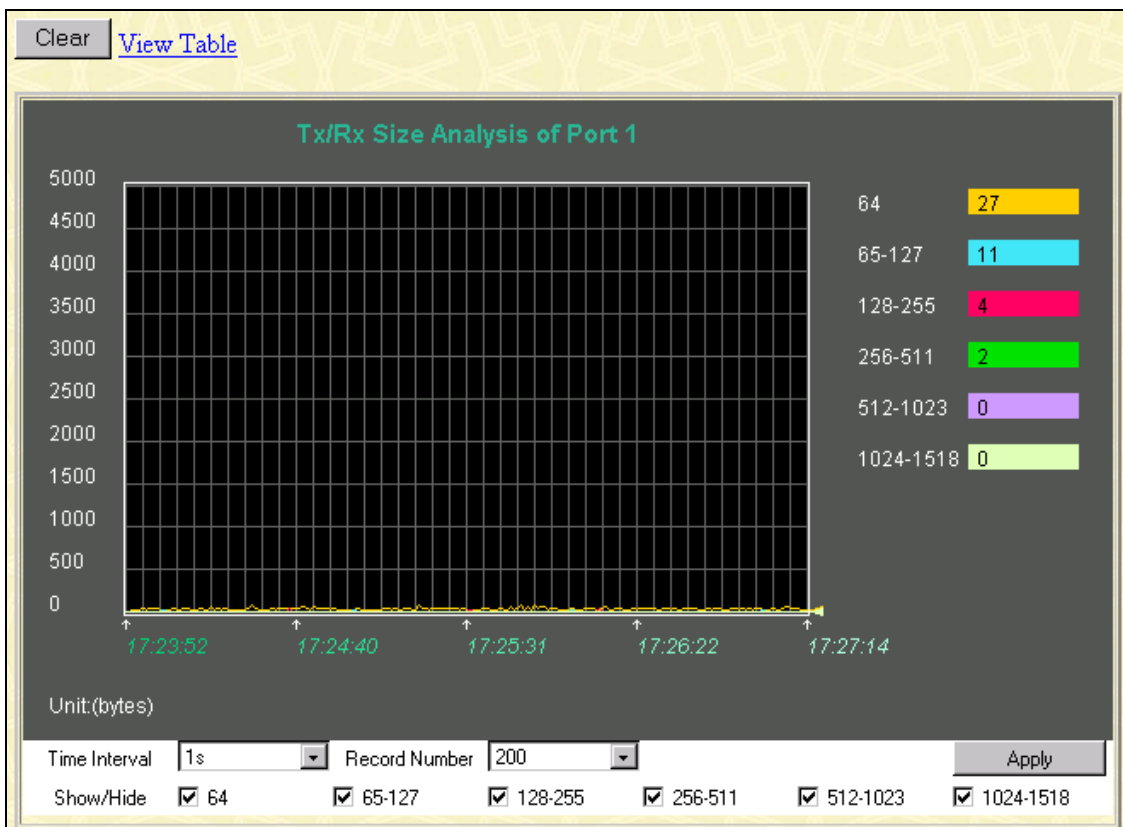


Figure 7-62. Tx/Rx Size Analysis window (Line Chart)

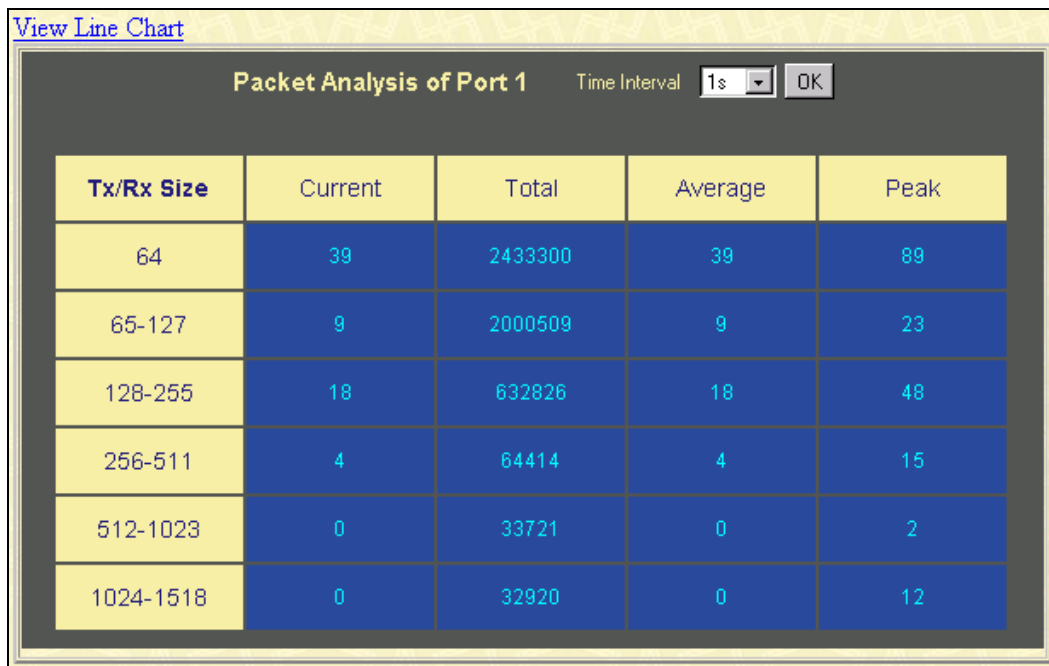


Figure 7-63. Packet Analysis window (Table)

The information is described as follows:

Time Interval [1s] – Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.

Record Number [200] – Select number of times the Switch will be polled between 20 and 200. The default value is 200.

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

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

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

256-511 – The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

512-1023 – The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

1024-1518 – The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Show/Hide – Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.

Clear – Clicking this button clears all statistics counters on this window.

View Table – Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart – Clicking this button instructs the Switch to display a line graph rather than a table.

MAC Address

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

Search by VLAN ID		<input type="text"/>	Jump	Find
Search by MAC Address		<input type="text" value="00-00-00-00-00-00"/>	Jump	Find
Search by Port		Port 1 ▾	Jump	Find
			Clear All	Clear By Port
MAC Address Table				
VID	MAC Address	Port	Learned	
1	00-00-81-01-00-01	1	dynamic	
1	00-00-81-05-00-01	1	dynamic	
1	00-00-81-48-70-01	1	dynamic	
1	00-00-81-48-76-00	1	dynamic	
1	00-00-81-b6-52-a6	1	dynamic	
1	00-00-81-e9-50-01	1	dynamic	
1	00-00-86-47-47-58	1	dynamic	
1	00-00-aa-cc-aa-cc	1	dynamic	
1	00-00-e2-61-53-18	1	dynamic	
1	00-00-e2-6b-bc-f6	1	dynamic	
1	00-00-e2-7f-6b-53	1	dynamic	
1	00-00-e2-82-7d-90	1	dynamic	
1	00-01-02-03-04-00	1	dynamic	
1	00-01-30-10-2c-c7	1	dynamic	
1	00-01-30-fa-5f-00	1	dynamic	
1	00-01-53-00-41-72	1	dynamic	
1	00-02-3f-70-d8-fe	1	dynamic	
1	00-02-3f-71-3e-ce	1	dynamic	
1	00-03-47-70-2c-ce	1	dynamic	
1	00-03-6d-1e-76-79	1	dynamic	
Total Addresses in Table: 508				Next

Figure 7-64. MAC Address Table window

The information is described as follows:

Search by VLAN ID – Allows the forwarding table to be browsed by VLAN ID (VID).

Search by MAC Address – Allows the forwarding table to be browsed by MAC Address.

Search by Port – Allows the forwarding table to be browsed by port number.

Jump – Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.

Find – Click the icon to find the data entry.

Clear All – Clears all forwarding table entries.

Clear By Port – Clears the forwarding table entries that have the entered port number.

VID – The VLAN ID of the VLAN the port is a member of.

MAC Address – The MAC address entered into the address table.

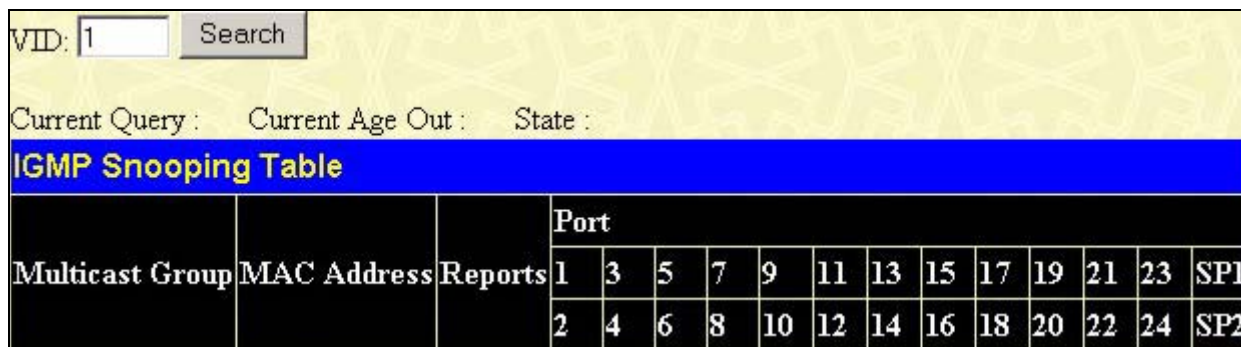
Port – The port that the MAC address above corresponds to.

Learned – How the switch discovered the MAC address. The possible entries are *Dynamic*, *Self*, and *Static*.

Next – Click this button to view the next page of the address table.

IGMP Snooping

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



VID: <input type="text" value="1"/> <input type="button" value="Search"/>		Current Query : Current Age Out : State :														
IGMP Snooping Table																
Multicast Group	MAC Address	Reports	Port													
			1	3	5	7	9	11	13	15	17	19	21	23	SP1	
			2	4	6	8	10	12	14	16	18	20	22	24	SP2	

Figure 7-65. IGMP Snooping Table window

The information is described as follows:

VID –VLAN ID of the VLAN for which the IGMP Snooping table is to be displayed.

Search – Click on the View button to display the IGMP Snooping Table for the current VID.

Multicast Group – The IP address of a multicast group learned by IGMP snooping.

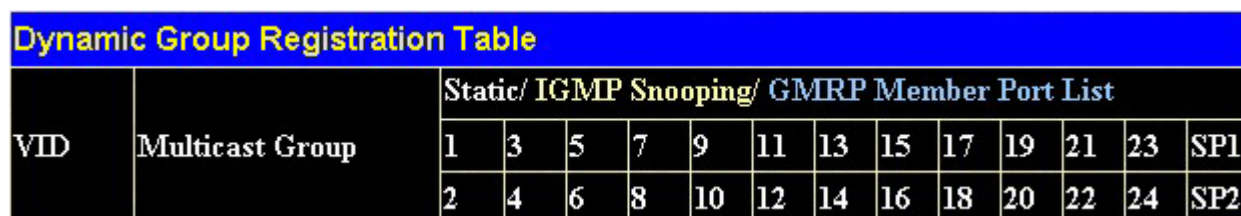
MAC Address – The corresponding MAC address learned by IGMP snooping.

Reports – The number of IGMP reports for the listed source.

Port Map – Displays the ports that have forwarded multicast packets.

Dynamic Group Registration

This read-only table contains filtering information for VLANs configured into the bridge by (local or network) management, or learned dynamically, specifying the set of ports to which frames received on a VLAN for this FDB and containing a specific Group destination address are allowed to be forwarded.



Dynamic Group Registration Table															
VID	Multicast Group	Static/ IGMP Snooping/ GMRP Member Port List													
		1	3	5	7	9	11	13	15	17	19	21	23	SP1	
		2	4	6	8	10	12	14	16	18	20	22	24	SP2	

Figure 7-66. Dynamic Group Registration Table window

VLAN Status

This read-only table displays VLAN multicast information.

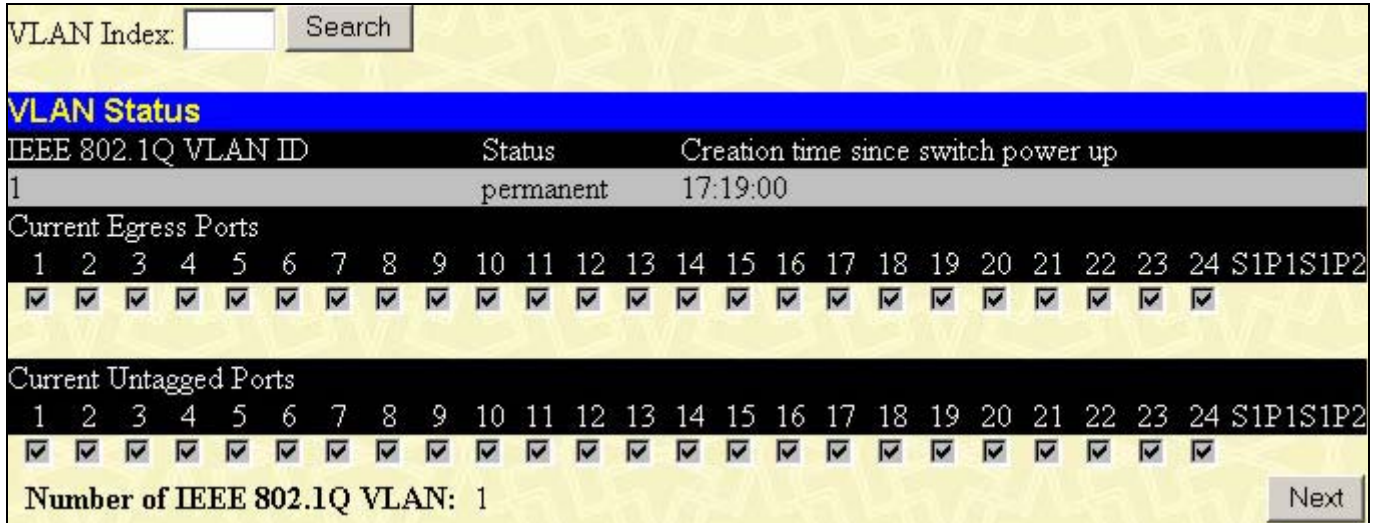


Figure 7-67. VLAN Status window

The information is described as follows:

VLAN Index –VLAN ID of the VLAN for which the multicast table is displayed.

Multicast Group – The IP address of a multicast group learned through multicasting.

Static Port List – Displays the ports that have forwarded multicast packets.

Port Access Control

There are five windows that comprise the 802.1X port-based authentication section.

Authenticator State

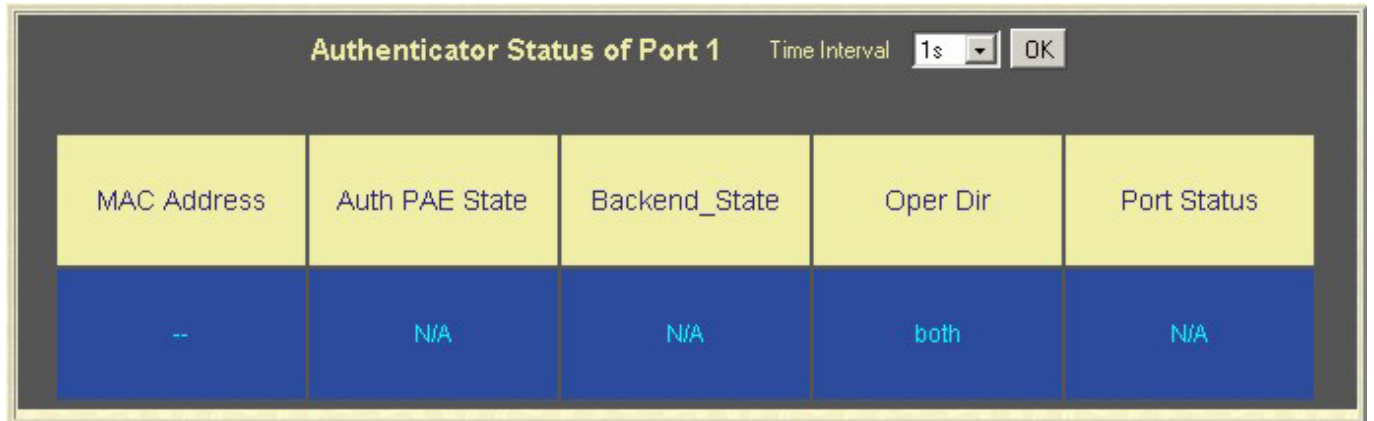


Figure 7-68. Authenticator Status window

This window displays the Authenticator Status for an individual port. To select a port, click a port on the front panel display. A polling interval between 1 and 60 seconds can be set using the drop-down menu at the top of the window.

The information on this window is described as follows:

MAC Address – The MAC address entered into the table.

Auth PAE State – The Authenticator PAE state value can be: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth*, or *N/A*. *N/A* (Not Available) indicates that the port's authenticator capability is disabled.

Backend State – The Backend Authentication state can be *Request, Response, Success, Fail, Timeout, Idle, Initialize*, or *N/A*. *N/A* indicates that the port's authenticator capability is disabled.

PortStatus – Auth Controlled Port Status can be *Authorized, Unauthorized*, or *N/A*.

Authenticator Statistics

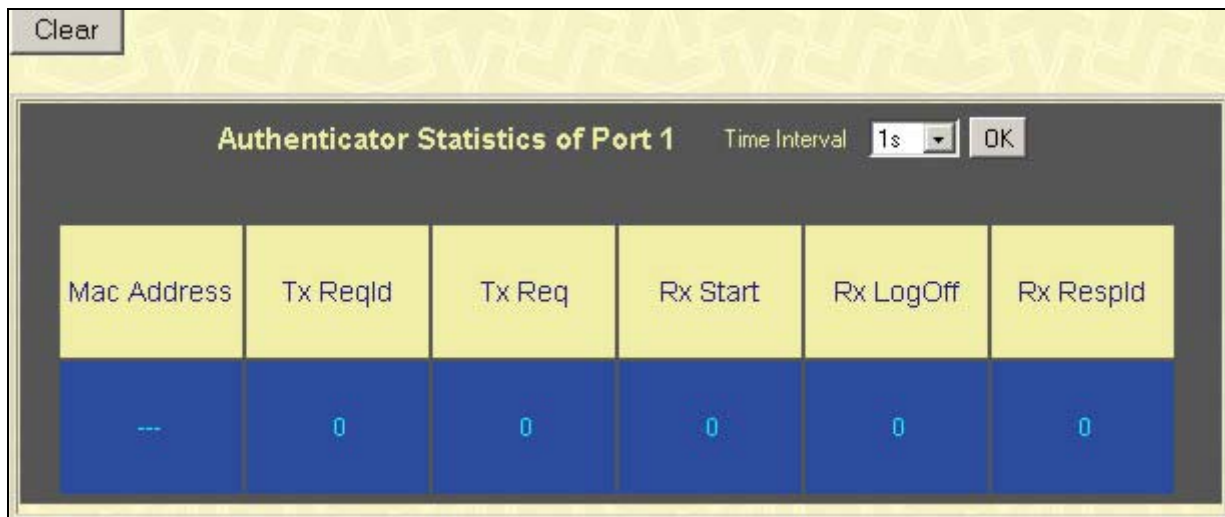


Figure 7-69. Authenticator Statistics window

This window displays the Authenticator Statistics for an individual port. To select a port, click a port on the front panel display. A polling interval between 1 and 60 seconds can be set using the drop-down menu at the top of the window. Clicking the **Clear** button resets these statistics counters.

The information on this window is described as follows:

Tx ReqId – The number of EAP Req/Id frames that have been transmitted by this Authenticator.

Tx Req – The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Rx Start – The number of EAPOL Start frames that have been received by this Authenticator.

Rx Logoff – The number of EAPOL Logoff frames that have been received by this Authenticator.

Rx RespId – The number of EAP Resp/Id frames that have been received by this Authenticator.

Authenticator Session-Counter

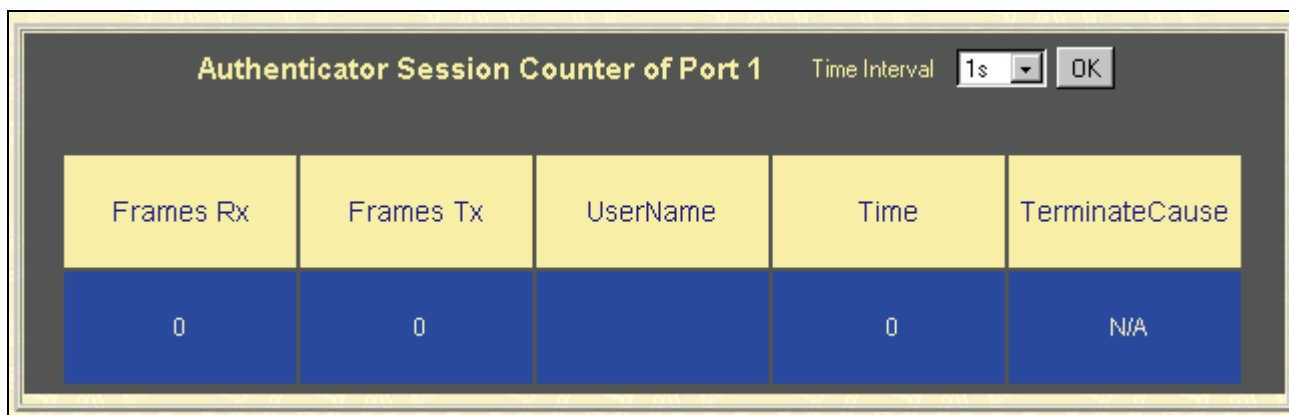


Figure 7-70. Authenticator Session Counter window

This window displays the Authenticator Session Counter for an individual port. To select a port, click a port on the front panel display. A polling interval between 1 and 60 seconds can be set using the drop-down menu at the top of the window.

The information on this window is described as follows:

Frames Rx – The number of user data frames received on this Port during the session.

Frames Tx – The number of user data frames transmitted on this Port during the session.

UserName – The User Name representing the identity of the client PAE.

Time – The session time is the duration of time in seconds.

TerminateCause – The reason for the session termination. This parameter can take the following values: Client Logoff, Port Failure, Client Restart, Reauthentication Failure, AuthControlledPortControl set to ForceUnauthorized, Port Re-initialization, Port Administratively Disabled, and Not Terminated Yet.

Radius Authentication

Server	UDP Port	Timeouts	Requests	Challenges	Accepts	Rejects
N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A

Figure 7-71. Radius Authentication window

This window displays Radius Authentication information. A polling interval between 1 and 60 seconds can be set using the drop-down menu at the top of the window.

The information on this window is described as follows:

Server – The remote RADIUS server IP address.

UDP Port – The UDP socket port numbers of the RADIUS server.

Timeouts – The counter of timeouts from RADIUS authentication.

Requests – The counter of access requests from RADIUS authentication.

Challenges – The counter of access challenges from RADIUS authentication.

Accepts – The counter for the number of acceptances from RADIUS authentication.

Rejects – The counter for the number of rejections from RADIUS authentication.

Radius Accounting



Figure 7-72. Radius Accounting window

This window displays Radius Accounting information. A polling interval between 1 and 60 seconds can be set using the drop-down menu at the top of the window.

The information on this window is described as follows:

Server IP Addr – The IP address of the RADIUS accounting server.

UDP Port – The UDP socket port number of the RADIUS accounting server.

Timeouts – The counter of the timeout connections to the RADIUS accounting server.

Requests – The counter of the requests from the RADIUS accounting server.

Responses – The counter for the number of rejections from RADIUS accounting server.

Maintenance

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

TFTP Services

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

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

Update Firmware

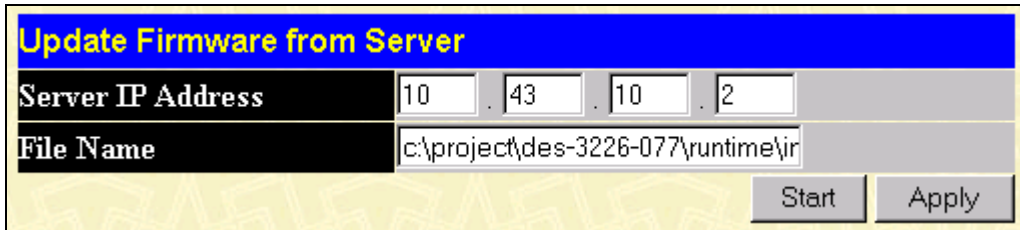


Figure 7-73. Update Firmware from Server window

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

The information is described as follows:

Server IP Address – The IP address of the TFTP server.

File Name – The full file name (including path) of the new firmware file on the TFTP server.

Configuration File

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

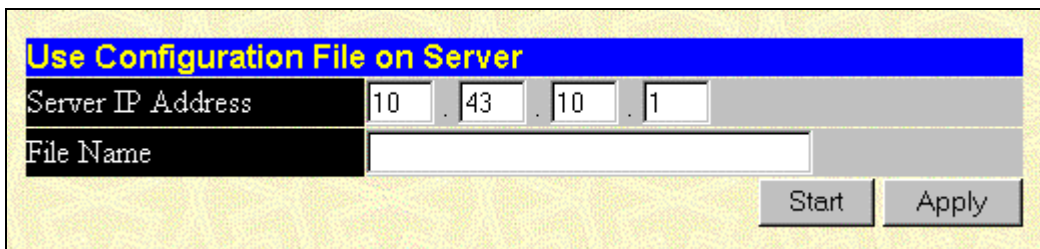


Figure 7-74. Use Configuration File on Server window

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

The information is described as follows:

Server IP Address – The IP address of the TFTP server.

File Name – The full file name (including path) of the new firmware file on the TFTP server.

Note: Configuration files used in the earlier version of this switch (firmware version 1.0) are not supported by the present version (firmware version 2.0). The Switch Information window displays the firmware version.

Save Settings

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

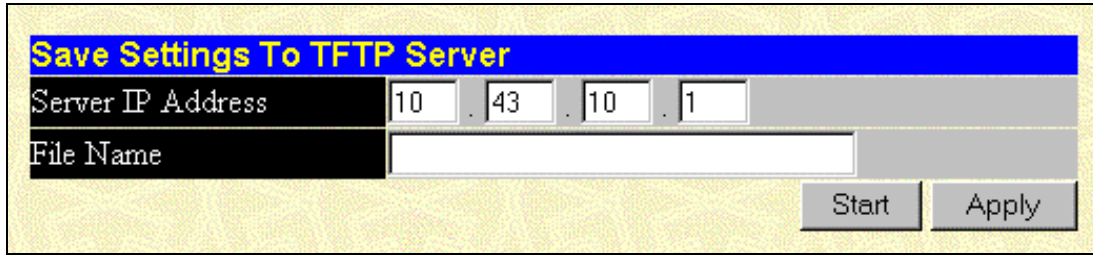


Figure 7-75. Save Settings To TFTP Server window

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

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

The information is described as follows:

Server IP Address – The IP address of the TFTP server.

File Name – The full file name (including path) of the new firmware file on the TFTP server.

Save History Log

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

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

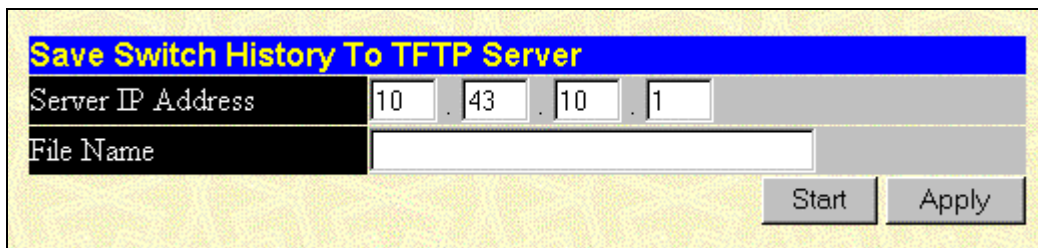


Figure 7-76. Save Switch History To TFTP Server window

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

The information is described as follows:

Server IP Address – The IP address of the TFTP server.

File Name – The full file name (including path) of the new firmware file on the TFTP server.

Download Hostkey Certificate

This window is used for downloading a hostkey for the SSH(Security Shell) function.

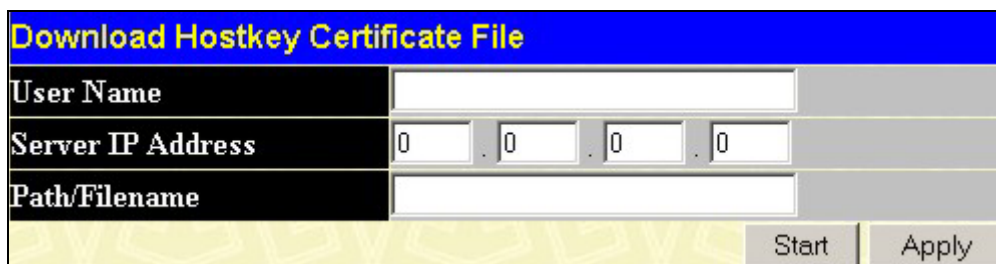


Figure 7-77. Download Hostkey Certificate window

To download the Hostkey Certificate file, modify the following fields and press APPLY and then START.

Username: [] – Enter the username that was applied in the SSH (Security Shell) settings.

Server IP Address: [] – Enter the IP address of the server where the file is being downloaded from.

Path/Filename: [] – Enter the name of the path to be downloaded. Note that the file must be a .cer file.

Switch History

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

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

Figure 7-78. Switch History window

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

The information is described as follows:

Sequence – A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.

Time – Displays the time in days, hours, and minutes since the Switch was last restarted.

Log Text – Displays text describing the event that triggered the history log entry.

Ping Test

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

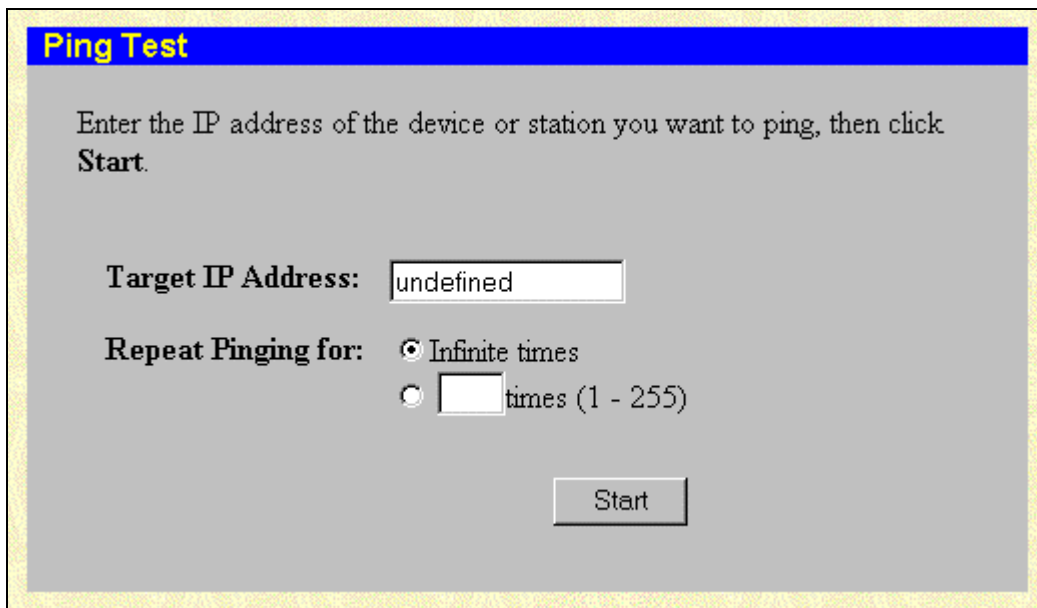


Figure 7-79. Ping Test window

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

Save Changes

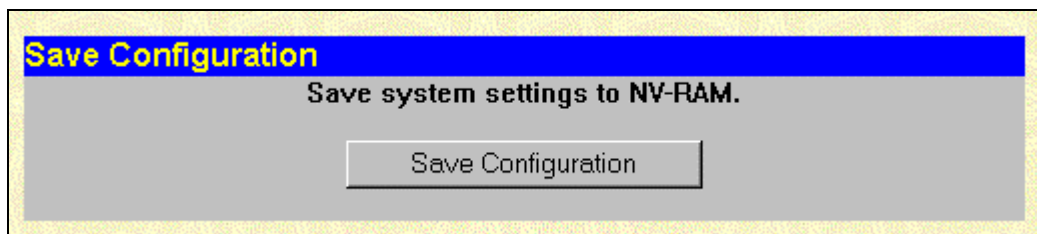


Figure 7-80. Save Configuration window

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

Factory Reset

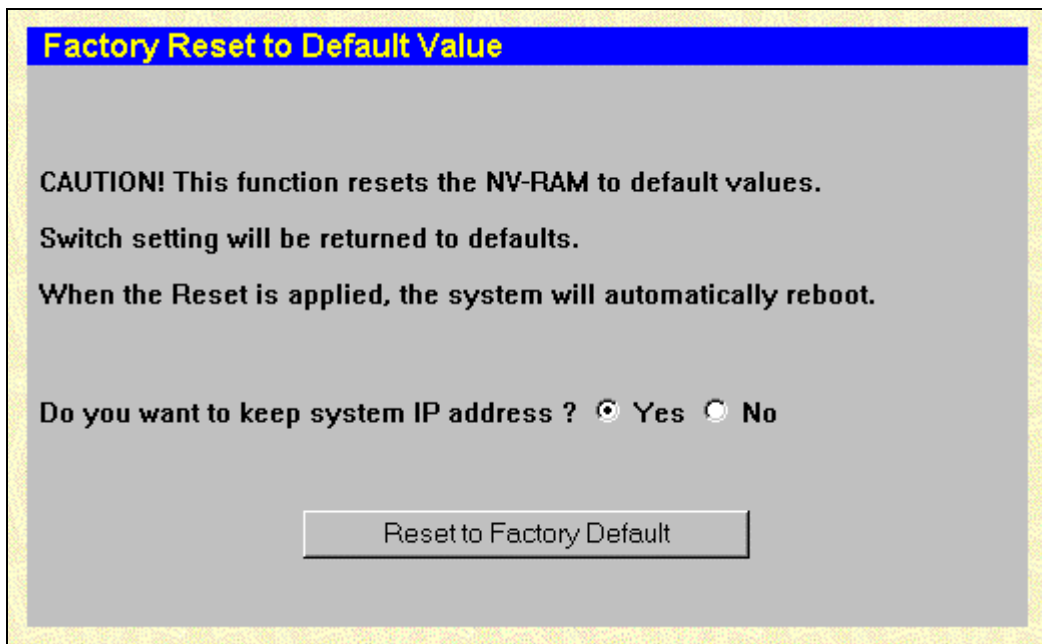


Figure 7-81. Factory Reset to Default Value window

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

Restart System

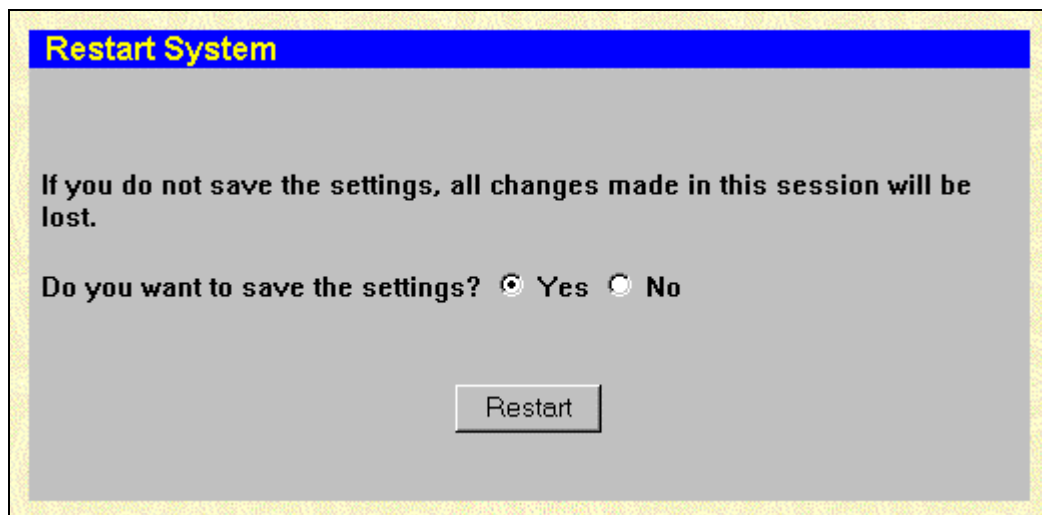


Figure 7-66. Restart System window

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

Connection Timeout

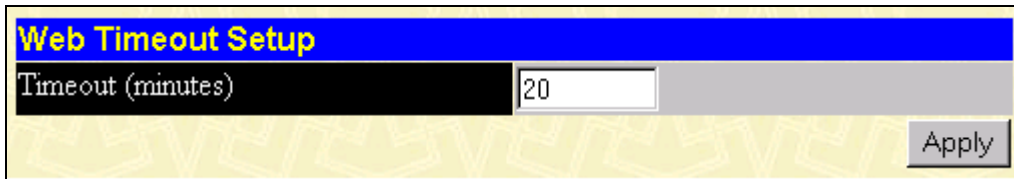


Figure 7-67. Web Timeout Setup window

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

Logout

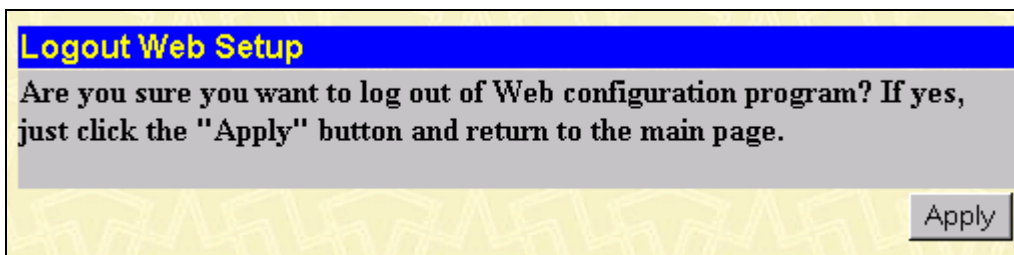


Figure 7-68. Logout Web Setups window

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

Help

Click this button to access the online helpfiles for the Switch.



TECHNICAL SPECIFICATIONS

General									
Standards:	IEEE 802.3ab Gigabit Ethernet IEEE 802.3ad Port Trunking IEEE 802.3z Gigabit Ethernet IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.1p Priority Queue IEEE 802.1 Q VLAN IEEE 802.1D Spanning Tree IEEE 802.1w Rapid Spanning Tree IEEE 802.1x Port Control IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 NWay auto-negotiation								
Protocols:	CSMA/CD								
Data Transfer Rates: Ethernet Fast Ethernet	<table border="0"> <tr> <td>Half-duplex</td> <td>Full-duplex</td> </tr> <tr> <td>10 Mbps</td> <td>20Mbps</td> </tr> <tr> <td>100Mbps</td> <td>200Mbps</td> </tr> <tr> <td>1000Mbps</td> <td>2000Mbps</td> </tr> </table>	Half-duplex	Full-duplex	10 Mbps	20Mbps	100Mbps	200Mbps	1000Mbps	2000Mbps
Half-duplex	Full-duplex								
10 Mbps	20Mbps								
100Mbps	200Mbps								
1000Mbps	2000Mbps								
Topology:	Star								
Network Cables: 10BASE-T: 100BASE-TX:	2-pair UTP Cat. 3, 4, 5 (100 m) EIA/TIA- 568 100-ohm STP (100 m) 2-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)								
Number of Ports:	8 x 10/100 Mbps NWay ports (DHS-3210)								

General	
	16 x 10/100 Mbps NWay ports (DHS-3218) 24 x 10/100 Mbps NWay ports (DHS-3226) 1 or 2 100BASE ports or 2 1000BASE ports (optional)

Physical and Environmental	
AC inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	40 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
Weight:	2.8 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(CNS13438)
Safety:	UL/CUL TUV/GS

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	8 Mbytes per device
Filtering Address Table:	8K
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 14,880 pps per port (for 10M) 148,800 pps per port (for 100Mbps) 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10–1000000 seconds. Default = 300.

B

RJ-45 PIN SPECIFICATION

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

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

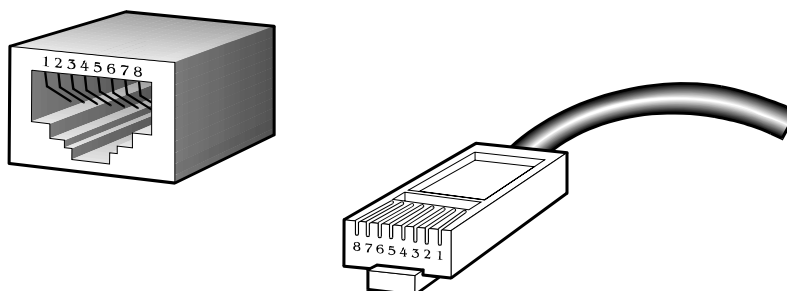


Figure B-1. The standard RJ-45 receptacle/connector

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

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



RUNTIME SWITCHING SOFTWARE DEFAULT SETTINGS

Load mode	Ethernet
Configuration update	Disable
Firmware update	Disable
Out-of-band baud rate	9600
RS232 mode	Console
IP address	10.90.90.90
Subnet mask	255.0.0.0
Default gateway	0.0.0.0
BootP service	Disable
TFTP server IP address	0.0.0.0
Auto log-out	10 min
User name	None
Password	None
MAC address aging time	300 secs
IGMP snooping	Disable
Switch GVRP	Disable
Telnet status	Enable
Web status	Enable
Device STP	Disable
Port STP	Enable
Port enable	Enable
Group address filter mode	Forward all unregistered
Scheduling mechanism for COS queues	Strict
Trunk Load Sharing Algorithm	Src Address
GMRP	Disable
Filtering EAPOL PDU	Yes
Bridge max age	20 secs
Traffic Segmentation	Disable
Bridge hello time	2 secs
Bridge forward delay	15 secs
Bridge priority	32768

Port STP cost	100
Port STP priority	128
NWay	Enable
Community string	"public", "private"
VLAN mode	IEEE 802.1Q
Management VLAN ID	1
Default port VID	1
Ingress rule checking	Disable
Device 802.1X	Disable
Port 802.1X Capability	None

UNDERSTANDING AND TROUBLESHOOTING THE SPANNING TREE PROTOCOL

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

The port is put into the listening state where it receives BPDUs and passes them to the switch's CPU. BPDU packets from the CPU are processed. If no BPDUs that suggest the port should go to the blocking state are received:

The port waits for the expiration of the forward delay timer. It then moves to the learning state.

In the learning state, the port learns station location information from the source address of packets and adds this information to its forwarding database.

The expiration of forwarding delay timer moves the port to the forwarding state, where both learning and forwarding are enabled. At this point, packets are forwarded by the port.

Blocking State

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

A port in the blocking state does the following:

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

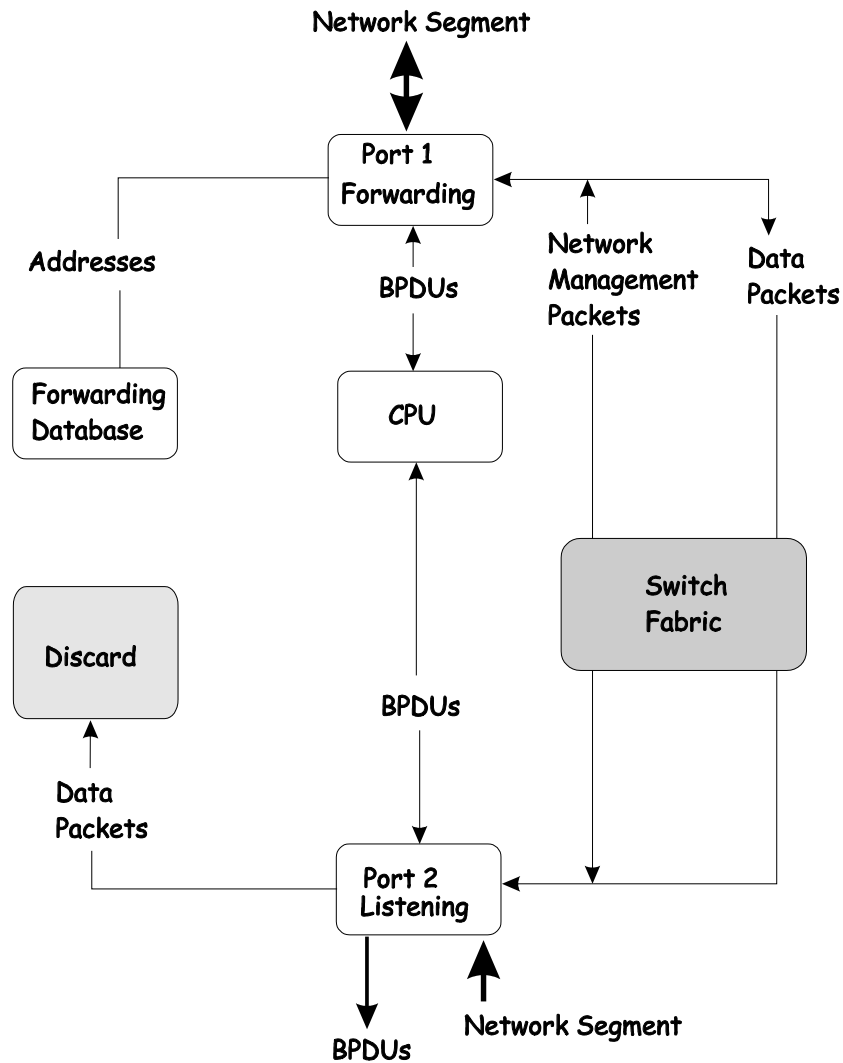
Listening State

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

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

- A port in the listening state does the following:
- Discards frames received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database

- Receives BPDUs and directs them to the CPU.
- Processes BPDUs received from the CPU.
- Receives and responds to network management messages.

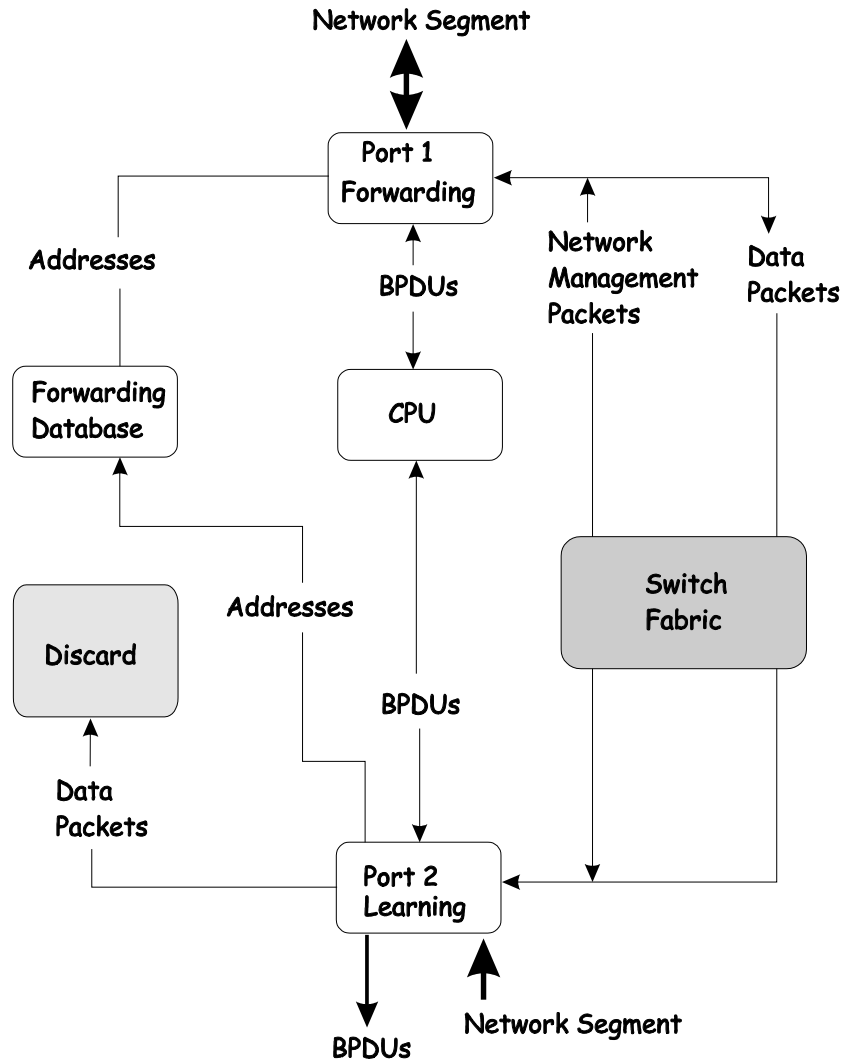


Learning State

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

A port in the learning state does the following:

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

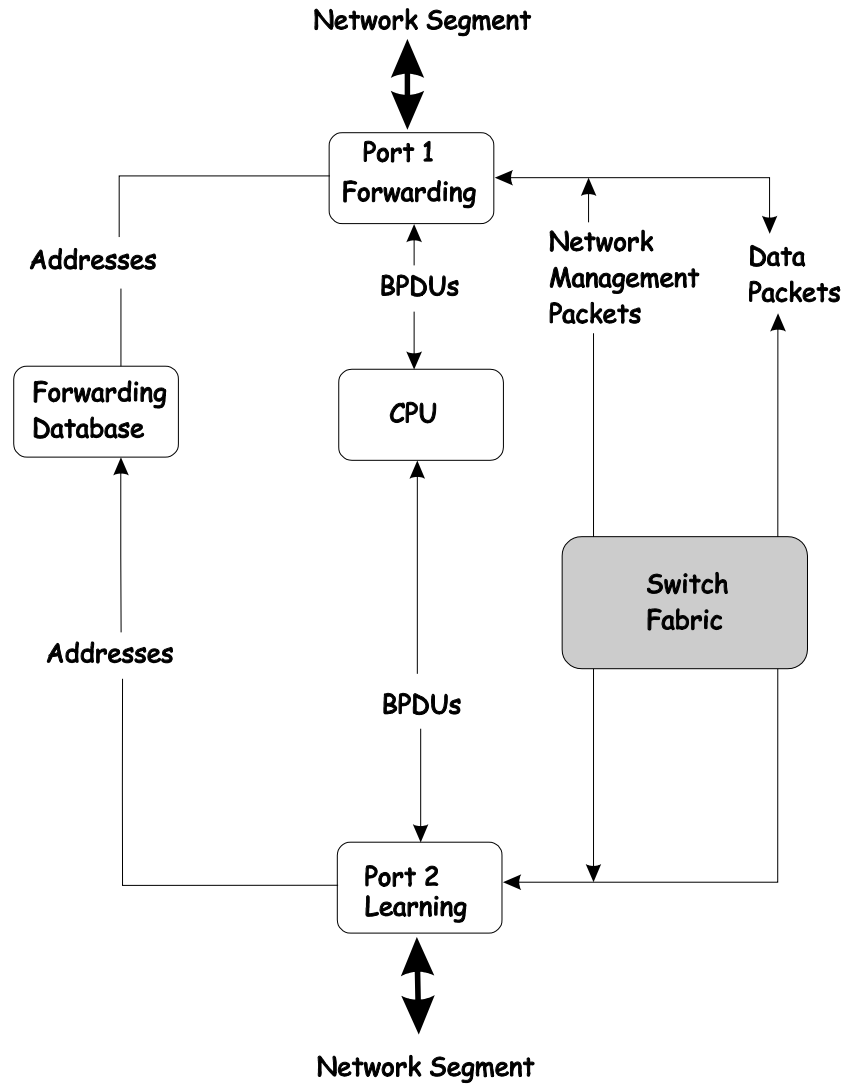


Forwarding State

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

A port in the forwarding state does the following:

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

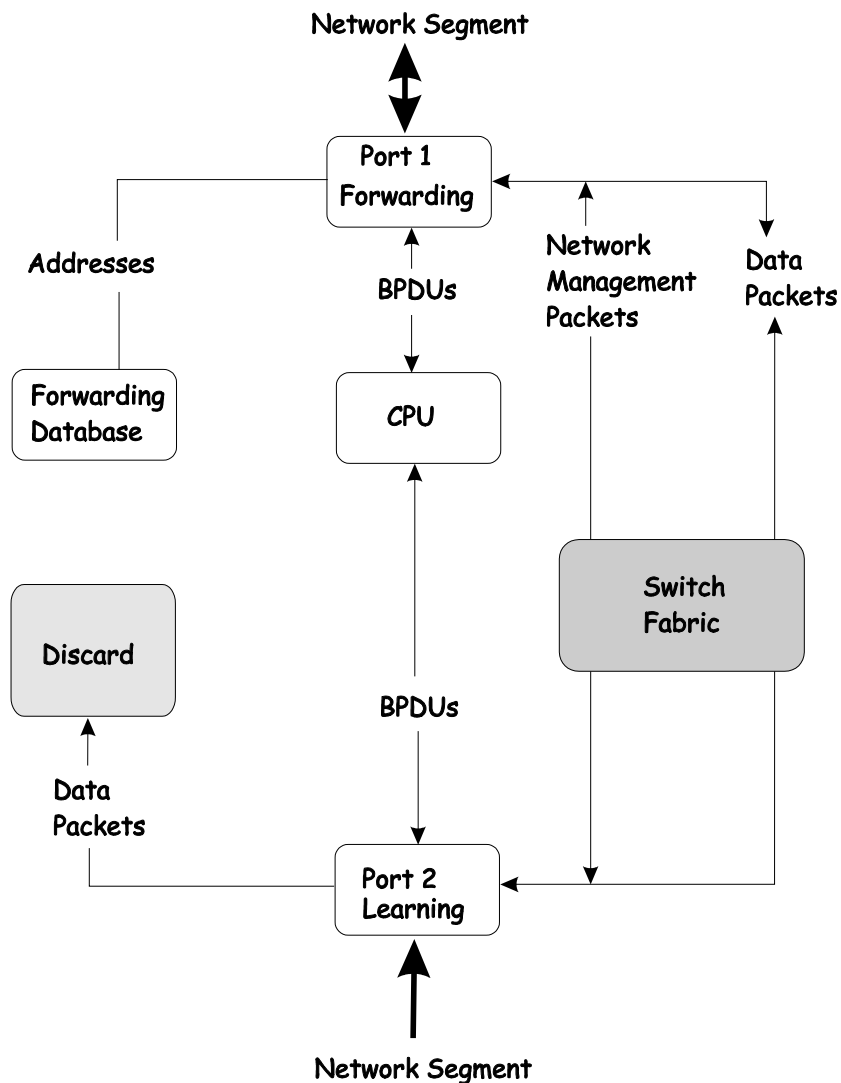


Disabled State

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

A disabled port does the following:

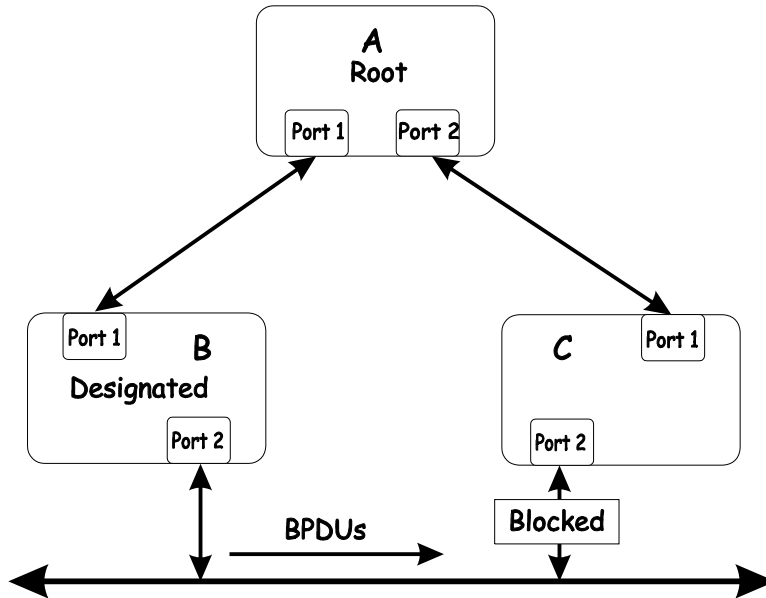
- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs, but does not direct them to the system CPU.
- Does not receive BPDUs for transmission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



Troubleshooting STP

Spanning Tree Protocol Failure

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



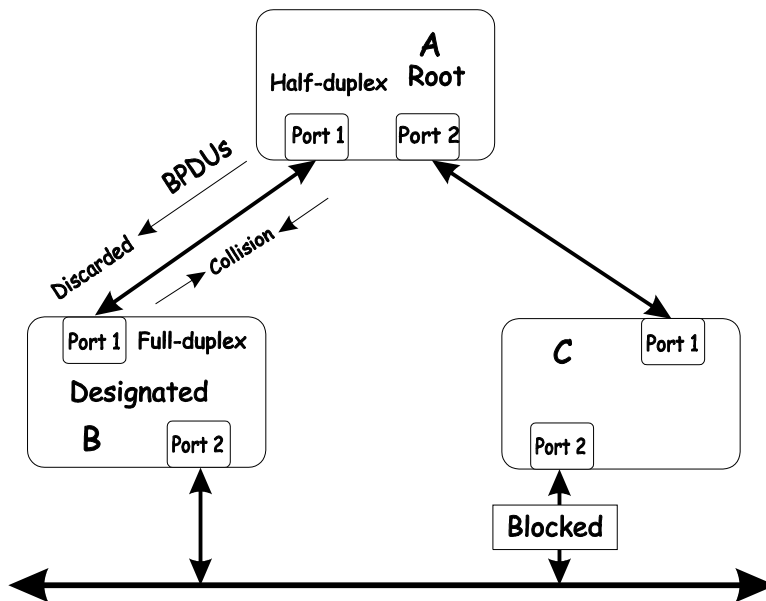
In this example, B has been elected as the designated bridge and port 2 on C is in the blocking state. The election of B as the designated bridge is determined by the exchange of BPDUs between B and C. B had a better BPDU than C. B continues sending BPDUs advertising its superiority over the other bridges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

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

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

Full/Half Duplex Mismatch

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

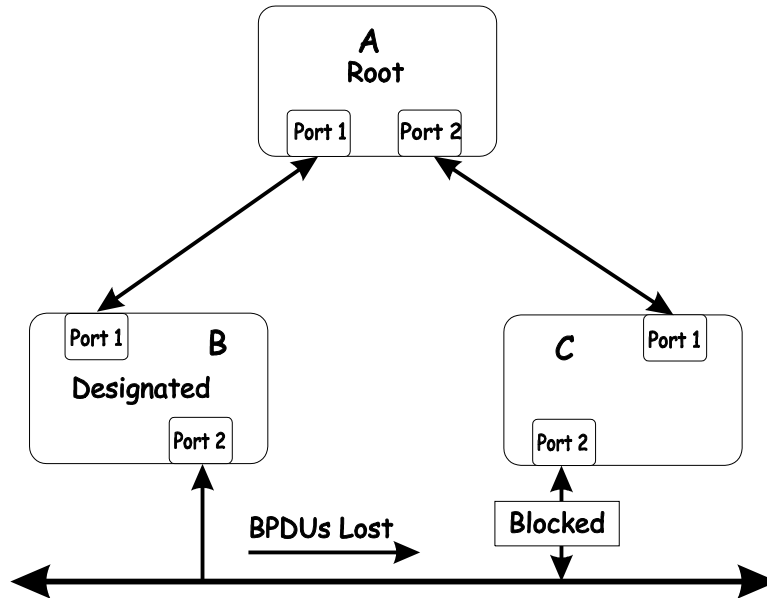


In the above example, port 1 on B is configured as a full-duplex port and port 1 on A is either configured as a half-duplex port, or left in auto-negotiation mode. Because port 1 on B is configured as a full-duplex port, it does not do the carrier sense when accessing the link. B will then start sending packets even if A is using the link. A will then detect collisions and begin to run

the flow control algorithm. If there is enough traffic between B and A, all packets (including BPDUs) will be dropped. If the BPDUs sent from A to B are dropped for longer than the MAX AGE, B will lose its connection to the root (A) and will unblock its connection to C. This will lead to a data loop.

Unidirectional Link

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



In this example, port 2 on B can receive but not transmit packets. Port 2 on C should be in the blocking state, but since it can no longer receive BPDUs from port 2 on B, it will transition to the forwarding state. If the failure exists at boot, STP will not converge and rebooting the bridges will have no effect. (Note: Rebooting would help temporarily in the previous example).

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

Packet Corruption

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

Resource Errors

The DES-3210/DES-3218/DES-3226 performs its switching and routing functions primarily in hardware, using specialized ASICs. STP is implemented in software and is thus reliant upon the speed of the CPU and other factors to converge. If the CPU is over-utilized, it is possible that BPDUs may not be sent in a timely fashion. STP is generally not very CPU intensive and is given priority over other processes, so this type of error is rare.

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

Identifying a Data Loop

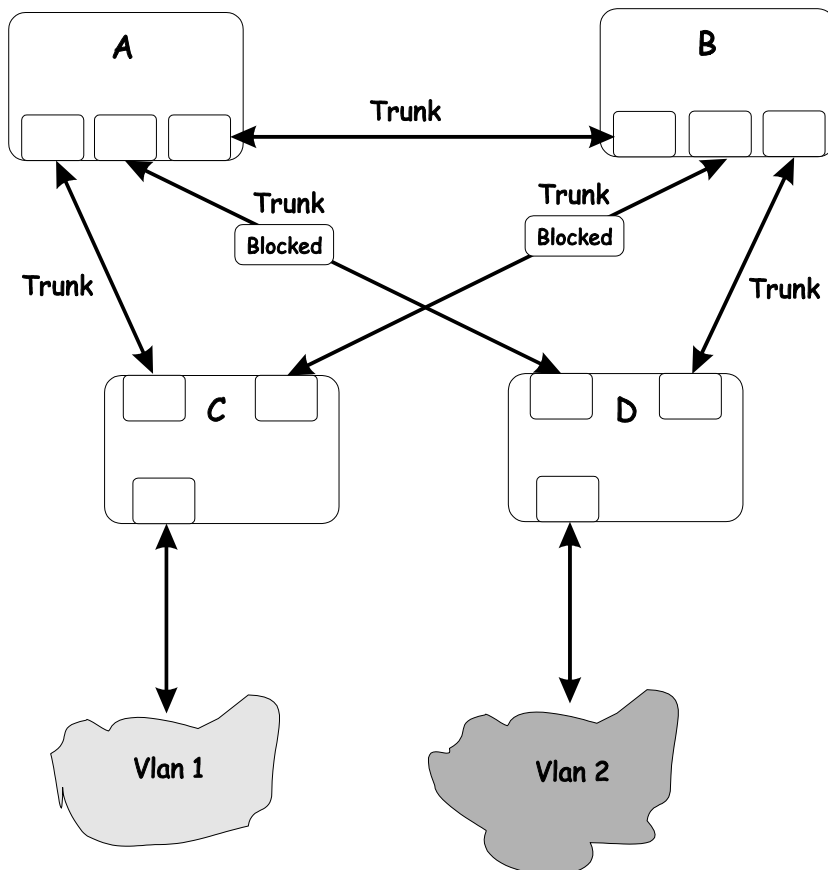
Broadcast storms have a very similar effect on the network to data loops, but broadcast storm controls in modern switches have (along with subnetting and other network practices) have been very effective in controlling broadcast storms. The best way to determine if a data loop exists is to capture traffic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

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

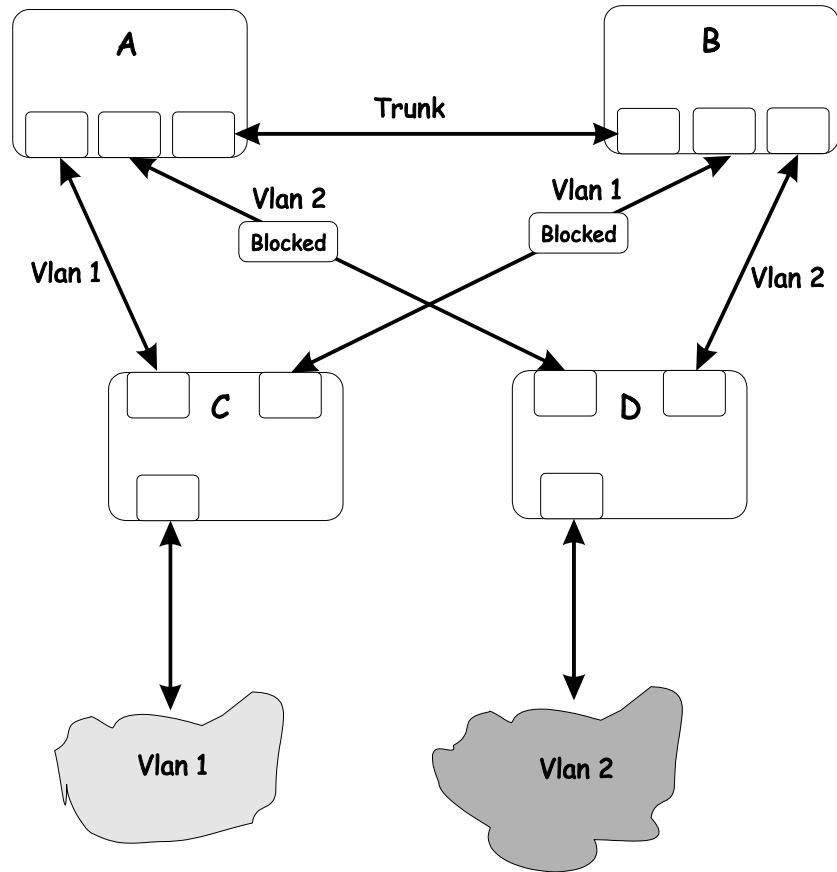
The priority for most cases is to restore connectivity as soon as possible. The simplest remedy is to manually disable all of the ports that provide redundant links. Disabling ports one at a time, and then checking for a restoration of the user's connectivity will identify the link that is causing the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

Avoiding Trouble

- Know where the root is located.
- Although the STP can elect a root bridge, a well-designed network will have an identifiable root for each VLAN. Careful setup of the STP parameters will lead to the selection of this best switch as the root for each VLAN. Redundant links can then be built into the network. STP is well suited to maintaining connectivity in the event of a device failure or removal, but is poorly suited to designing networks.
- Know which links are redundant.
- Organize the redundant links and tune the port cost parameter of STP to force those ports to be in the blocking state.
- For each VLAN, know which ports should be blocking in a stable network. A network diagram that shows each physical loop in the network and which ports break which loops is extremely helpful.
- Minimize the number of ports in the blocking state.
- A single blocking port transitioning to the forwarding state at an inappropriate time can cause a large part of a network to fail. Limiting the number of blocked ports help to limit the risk of an inappropriate transition.



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



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



BRIEF REVIEW OF BITWISE LOGICAL OPERATIONS

AND

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

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

OR

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

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

XOR

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

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

NOT

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

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

INDEX

A	
AC inputs	164
AC power cord	5
Access Rights	
read only	80, 131
read/write	80, 131
Accessory pack	5
Administrator	34
Aging Time, definition of	17
Aging Time, range of	17
APPLY	33
Automatic learning	18
auto-negotiate	2
B	
BOOTP protocol	41
BOOTP server	41
Bridge Forward Delay	22
Bridge Hello Time	22, 47
Bridge Max. Age	22, 47
Bridge Priority	22, 47
broadcast domains	24
C	
Changing your Password	39
Community Name	16
Community name, definition of	79
Community names	
Private	79
Public	79
Connecting to the Switch	
VT100-compatible terminal	32
Connections	
Switch to End Node	13
Switch to Hub or Switch	13
console	32
Console	12
console port	2, 8
Console port (RS-232 DCE)	14
Console port settings	14
Create/Modify User Accounts	39
D	
Data filtering	2
Data filtering rate	2
Data forwarding	2
Data forwarding rate	2
Default Gateway	41
Diagnostic port	2
Dimensions	164
Dynamic filtering	18
E	
Egress port	24
End Node	13
F	
factory reset	37
Filtering	18
Flash memory	3
Forwarding	17
Front Panel	8
Full-duplex	2
G	
gateway router	15
General User	35
H	
half-duplex	2
Humidity	164
I	
IEEE 802.1Q tagging	24
IEEE 802.1Q VLANs	24
Illustration of STA	22
Ingress port	24, 27
Internet Group Management Protocol (IGMP)	43, 101
IP address	81, 132
IP Address	15

IP Addresses and SNMP Community Names	15	refresh	33
IP Configuration	41	RJ-45 Pin Specification	166
L		RMON probe	56
LED Indicators	12	RS-232	2
log in	38	S	
Logging on	33	Save Changes	33
M		Saving Changes	36
MAC address filtering	18	Secure Shell (SSH)	68, 127
MAC Address Learning	164	security	16, 24
MAC-based VLANs	24	Setup	5
Main Menu	34, 35, 37, 38	sniffer	56
Management	3	SNMP Community String	80, 81, 131, 132
Management Information Base (MIB)	16	SNMP Manager Configuration	79, 131
Max. Age	22, 47	SNMP Manager Configuration parameter	
MIB	16	Status	80, 81, 131, 132
MIB objects	16	SNMP Security (Community Names)	79, 131
MIB-II	16	SNMP Trap Manager Configuration	79
MIBs	16	Spanning Tree Algorithm	3
mirror port	56	Spanning Tree Algorithm (STA)	18
module	2	Spanning Tree Protocol	18
Modules	9	Storage Temperature	164
Multicasting	43, 101	Store and forward switching	2
N		subnet mask	99
Network Classes		Subnet Mask	41
Class A, B, C for Subnet Mask	41	Super User	35
NV-RAM	36	T	
O		<i>tagging</i>	24
Operating Temperature	164	Tagging	24
Out-of-Band/Console Setting menu	44	TCP/IP Settings	41
P		Telnet	43, 101
password	33	TELNET	32
Port Mirroring	56	Terminal Access Controller Access Control System	
Port Priority	22, 48	(TACACS)	69, 129
port-based VLANs	24	terminal emulator	32
ports	2	terminal parameters	32
Power	12	Third-party vendors' SNMP software	17
Power Consumption	164	Transmission Methods	164
R		Trap managers	16
RAM	36	Trap Type	
RAM Buffer	164	Authentication Failure	16
Rear Panel	8	Cold Start	16

Link Change Event.....	16	username	33
New Root	16	V	
Topology Change	16	View based Access Control Model (VACM) 88, 137	
Warm Start	16	View/Delete User Accounts.....	39
Traps	16	VLAN	18, 24
U		VT100-compatible terminal.....	32
unauthorized users.....	33	W	
Unpacking	5	Web-based management	97
<i>untagging</i>	24	Web-based management module	97
Untagging	24	Weight	164
User Accounts Management	39		

D-Link Offices

Australia

D-Link Australia

1 Giffnock Avenue, North Ryde, NSW 2113,
Sydney, Australia
TEL: 61-2-8899-1800 FAX: 61-2-8899-1868
TOLL FREE (Australia): 1800-177100
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au & info@dlink.com.au

Brazil

D-Link Brasil Ltda.

Edifício Manoel Tabacow Hydal,
Rua Tavares Cabral 102 Sala 31, 05423-030
Pinheiros, Sao Paulo, Brasil
TEL: (55 11) 3094 2910 to 2920 FAX: (55 11) 3094 2921
E-MAIL: efreitas@dlink.cl

Canada

D-Link Canada

2180 Winston Park Drive, Oakville,
Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5095
TOLL FREE: 1-800-354-6522 URL: www.dlink.ca
FTP: [ftp.dlinknet.com](ftp://ftp.dlinknet.com) E-MAIL: techsup@dlink.ca

Chile

D-Link South America (Sudamérica)

Isidora Goyenechea 2934 Of. 702, Las Condes Fono,
2323185, Santiago, Chile, S. A.
TEL: 56-2-232-3185 FAX: 56-2-232-0923
URL: www.dlink.cl
E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl

China

D-Link China

15th Floor, Science & Technology Tower,
No.11, Baishiqiao Road, Haidan District, 100081 Beijing, China
TEL: 86-10-68467106 FAX: 86-10-68467110
URL: www.dlink.com.cn
E-MAIL: liweii@digitalchina.com.cn

Denmark

D-Link Denmark

Naverland 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: 202-245-6176 FAX: 202-245-6192
URL: www.dlink-me.com
E-MAIL: support@dlink-me.com & fateen@dlink-me.com

Finland

D-Link Finland

Pakkalankuja 7A, FIN-0150 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
URL: www.dlink.de
BBS: 49-(0) 6192-971199 (analog)
BBS: 49-(0) 6192-971198 (ISDN)
INFO: 00800-7250-0000 (toll free)
HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 E-MAIL: info@dlink.de

India

D-Link India

Plot No.5, Bandra-Kurla Complex Rd., Off Cst Rd.,
Santacruz (East), Mumbai, 400 098 India
TEL: 91-022-652-6696/6578/6623
FAX: 91-022-652-8914/8476
URL: www.dlink-india.com & www.dlink.co.in
E-MAIL: service@dlink.india.com & tushars@dlink-india.com

Italy

D-Link Mediterraneo Srl/D-Link Italia

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

Japan

D-Link Japan

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

Netherlands D-Link Benelux

Fellenoord 130 5611 ZB, Eindhoven, The Netherlands

TEL: 31-40-2668713 FAX: 31-40-2668666

URL: www.d-link-benelux.nl & www.dlink-benelux.be

E-MAIL: info@dlink-benelux.nl & info@dlink-benelux.be

Norway D-Link Norway

Waldemar Thranesgate 77, 0175 Oslo, Norway

TEL: 47-22-99-18-90 FAX: 47-22-20-70-39 SUPPORT: 800-10-610

URL: www.dlink.no

Russia D-Link Russia

Michurinski Prospekt 49, 117607 Moscow, Russia

TEL: 7-095-737-3389 & 7-095-737-3492

FAX: 7-095-737-3390 URL: www.dlink.ru

E-MAIL: vl@dlink.ru

Singapore D-Link International

1 International Business Park, #03-12 The Synergy,

Singapore 609917

TEL: 6-6774-6233 FAX: 6-6774-6322

E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

South Africa D-Link South Africa

Unit 2, Parkside, 86 Oak Avenue, Highveld Technopark,
Centurion, Gauteng, 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 (Spain and Portugal)

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@tsc.dlinktw.com.tw

Turkey**D-Link Middle East**

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

U.A.E.**D-Link Middle East**

CHS Aptec (Dubai), P.O. Box 33550 Dubai, United Arab Emirates
TEL: 971-4-366-885 FAX: 971-4-355-941
E-MAIL: Wxavier@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®