



DHS-3224V  
Ethernet over VDSL  
24-Port Switch  
*User's Guide*

---

---

First Edition August 2002)

---



RECYCLABLE

## Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätem 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 Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät ist 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 – Netzkabel 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, 0.75mm<sup>2</sup> einzusetzen.

## Trademarks

Copyright D-Link Corporation ©2001.  
Contents subject to change without prior notice.

## 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, as stipulated by the United States Copyright Act of 1976.

---

# Table Of Contents

---

<b>About This Guide</b> .....	<b>xiii</b>
Overview of this User's Guide.....	xiii
Intended Audience .....	xiii
Terminology.....	xiii
<b>Introduction</b> .....	<b>1</b>
Ethernet over VDSL.....	1
Applications .....	1
Hardware.....	2
<i>Switch Description and Function</i> .....	3
<i>Features</i> .....	4
Ports .....	4
Performance Features.....	4
Management.....	4
<b>Installation and Setup</b> .....	<b>5</b>
Unpacking .....	5
Switch Placement .....	5
Rack Installation .....	6
Power on .....	7
<b>Switch Components</b> .....	<b>8</b>
Front Panel .....	8
Rear Panel .....	8
LED Indicators.....	9
<b>Network Connections</b> .....	<b>10</b>
Connecting Multiple Switches .....	10
Stacking a Switch Group.....	10
Powering On Switch Stacks.....	11
Cable Connections for a Stacked Switch Group .....	11
<i>Front Panel Connections</i> .....	13
<i>Rear Panel Connections</i> .....	14
<i>Network Connections to DSL Splitter</i> .....	15
Cable Attachments to DSL Splitter.....	16
Install the Ground Wire on the DSL Splitter.....	17
Connection to End User .....	17
<b>Switch Management Concepts</b> .....	<b>18</b>
Local Console Management.....	18
IP Addresses and SNMP Community Names .....	19
Remote Management Setup Menu .....	20
MIBs .....	21
SNMP.....	22
Authentication.....	22
MAC Address Aging Time .....	22
Packet Filtering .....	22
Managing Switch Stacks.....	23
Determining Switch Stack Order .....	24
Spanning Tree Protocol.....	25

STP Operation Levels .....	25
Creating a Stable STP Topology .....	27
Illustration of STP .....	30
VLANs.....	31
IEEE 802.1Q VLANs.....	32
Asymmetric VLANs .....	37
<b>Configuring the Switch.....</b>	<b>38</b>
Connecting to the Switch .....	38
Console Usage Conventions.....	38
Connecting to the Switch Using Telnet.....	39
First Time Connecting to the Switch.....	39
User Accounts Management .....	40
Root, User+ and Normal User Privileges.....	42
<i>Save Changes</i> .....	42
Factory Reset.....	43
Logging On to The Switch Console.....	45
Updating or Deleting User Accounts .....	45
Viewing Current User Accounts .....	46
Deleting a User Account .....	46
<i>Configuring the Switch</i> .....	47
Serial Port and SLIP Settings .....	48
Switch Information .....	49
Stacking Configuration .....	50
System Information.....	51
Configure IP Address.....	52
Management Station IP Settings .....	53
Setting Trap Receivers .....	53
Configure Switch Settings.....	54
Switch Settings.....	54
Broadcast/Multicast Storm Control.....	55
Configure Ports .....	56
Configure Port Access Entity .....	59
PAE System Configuration .....	59
Configure 802.1X – Authenticator Configuration.....	61
Configure Radius Server .....	63
Configure Port Mirroring .....	65
VDSL Settings .....	65
Configure Spanning Tree Protocol.....	66
STP Parameter Settings.....	66
Port Spanning Tree Settings.....	67
MAC Address Filtering and Forwarding.....	68
Configure MAC Address Forwarding.....	68
Configure MAC Address Filtering.....	69
Configure Multicasting .....	69
Configure IEEE 802.1Q Multicast Forwarding .....	70
Configure IGMP Snooping .....	71
Configure VLANs.....	72
<i>Network Monitoring</i> .....	78
Port Utilization.....	78
Port Error Packets .....	78
Port Packet Analysis .....	79
Browse MAC Address .....	80
Switch History.....	80
<i>System Utilities</i> .....	81
Upgrade Firmware from TFTP Server .....	81
Use Configuration File on TFTP Server .....	82

Save Settings to TFTP Server .....	83
Save History Log to TFTP Server .....	83
Ping Test .....	84
Local Loopback Test .....	84
Line Loopback Test .....	85
<i>System Reboot</i> .....	86
Logout .....	87
<b>Using the Web Management Software .....</b>	<b>88</b>
Introduction .....	88
Getting Started .....	88
Log On to Web Manager .....	89
Web Interface Components .....	89
Accessing Menu Windows .....	90
<i>Switch Configuration</i> .....	91
System Information .....	91
System Time Setup .....	91
IP Settings .....	92
Switch Information .....	92
Stacking Configuration .....	93
Configure Ports .....	94
PAE System Control .....	98
Port Authenticating Settings .....	98
Initialize Ports(s) .....	99
Reauthenticate Ports(s) .....	99
Configure Authenticator .....	100
Radius Server .....	102
General Radius Server .....	102
Authentic Radius Server .....	103
Local User .....	104
Port Mirroring .....	104
Switch Settings .....	105
VDSL Settings .....	106
Configure 802.1Q Static VLANs .....	107
Add a Static 802.1Q VLAN .....	107
Edit 802.1Q VLANs .....	108
802.1Q Port Settings .....	109
Asymmetric VLANs .....	111
Multicasting Options .....	111
Group Address Filtering .....	111
Multicast Forwarding .....	112
IGMP Snooping .....	112
Priority .....	114
Spanning Tree Protocol Configuration .....	115
Port Spanning Tree .....	116
MAC Forwarding .....	117
MAC Filtering .....	117
Management .....	118
Management Station IP Settings .....	118
Community Strings .....	118
Trap Receivers .....	119
User Accounts .....	119
Serial Port Settings .....	121
<i>Monitoring</i> .....	123
Port Utilization .....	123
Packets .....	123
Received (RX) .....	124

---

UMB-cast (RX).....	125
Transmitted (TX) .....	127
Errors.....	128
Received (RX).....	128
Transmitted (TX) .....	130
Size.....	131
Packet Size .....	131
MAC Address .....	133
IGMP Snooping .....	134
Port Access Control .....	135
Authenticator State.....	135
Authenticator Statistics .....	135
Authenticator Session-Counter .....	136
Radius Authentication.....	136
Radius Accounting.....	137
<i>Maintenance.....</i>	<i>138</i>
TFTP Services.....	138
Update Firmware.....	138
Configuration File.....	138
Save Settings.....	139
Save History Log .....	139
Switch History.....	140
Ping Test .....	141
Local Loopback Test.....	141
Line Loopback Test .....	141
Save Changes .....	142
Factory Reset.....	142
Restart System.....	143
<b>Technical Specifications .....</b>	<b>144</b>
<i>Runtime Switching Software Default Settings.....</i>	<i>146</i>

**Rack Installation**

Figure 2-1. Attaching the mounting brackets to the Switch.....	6
Figure 2-2. Installing the Switch in an equipment rack .....	6

**Switch Components**

Figure 3-1. Front panel view of the Switch.....	8
Figure 3-2. Rear panel view of the Switch.....	8
Figure 3-3. The LED indicators .....	9

**Cables and Connections**

Figure 4-1. Switch Stack Connections .....	12
Figure 4-2. Front Panel Network Connections.....	13
Figure 4-3. Rear Panel Connections.....	14

**Management**

Figure 5-1. Boot Screen .....	19
Figure 5-2. Switch Information Screen .....	19
Figure 5-3. Remote Management Setup.....	20
Figure 5-4. Initial Stack Order .....	24
Figure 5-5. New Stack Order .....	24

**Console Configuration**

Figure 6- 1. Initial screen, first time connecting to the Switch .....	39
Figure 6- 2. Main menu (Access System Information Screen) .....	40
Figure 6- 3. Main Menu (Access User Accounts Menu).....	40
Figure 6- 4. Setup User Accounts Screen .....	41
Figure 6- 5. Main menu.....	43
Figure 6- 6. Save changes Screen .....	43
Figure 6- 7. Main Menu - Reboot .....	44
Figure 6- 8. System Reboot Menu .....	44
Figure 6- 9. Setup User Accounts Screen .....	45
Figure 6- 10. Serial Port and SLIP Settings Screen .....	48
Figure 6- 11. Switch Information Menu.....	49
Figure 6- 12. Stacking Configuration Screen – (Auto-detect) .....	50
Figure 6- 13. System Information Menu .....	51
Figure 6- 14. Setup System Time Menu .....	51
Figure 6- 15. Remote Management Setup Screen.....	52
Figure 6- 16. Setup Trap Recipients Menu .....	53
Figure 6- 17. Switch Settings Menu.....	54
Figure 6- 18. Configure Ports.....	56

---

Figure 6- 19. Configure Port Settings Screen.....	57
Figure 6- 20. Configure Port Security Screen .....	58
Figure 6- 21. PAE Configuration menu .....	59
Figure 6- 22. PAE System Configuration menu.....	59
Figure 6- 23. Port 802.1X Capability Settings screen.....	60
Figure 6- 24. Initialize Port(s) screen.....	60
Figure 6- 25. Reauthenticate Ports(s) menu .....	61
Figure 6- 26. Configure 802.1X – Authenticator Configuration screen.....	61
Figure 6- 27. Configure Radius Server menu.....	63
Figure 6- 28. Configure General Radius Server Setting screen .....	63
Figure 6- 29. Configure Authentic Radius Server screen.....	64
Figure 6- 30. Configure Local Users screen .....	64
Figure 6- 31. Setup Port Mirroring screen .....	65
Figure 6- 32. VDSL Settings Menu .....	66
Figure 6- 33. Configure Spanning Tree Menu .....	66
Figure 6- 34. Port Spanning Tree Settings Screen .....	67
Figure 6- 35. Unicast MAC Forwarding Screen .....	68
Figure 6- 36. MAC Address Filtering Screen .....	69
Figure 6- 37. Multicasting Menu Screen.....	69
Figure 6- 38. Multicast Forwarding Settings Screen.....	70
Figure 6- 39. IGMP Snooping Menu .....	71
Figure 6- 40. VLAN Menu.....	72
Figure 6- 41. Edit 802.1Q VLANs Menu.....	72
Figure 6- 42. Edit 802.1Q VLANs Menu.....	73
Figure 6- 43. VLAN Menu.....	74
Figure 6- 44. Configure 802.1Q Port Settings Screen.....	74
Figure 6- 45. Configure Asymmetric VLANs Menu .....	76
Figure 6- 46. Example Asymmetric VLAN Switch #1 .....	76
Figure 6- 47. Port Priority Screen .....	77
Figure 6- 48. Network Monitoring Menu.....	78
Figure 6- 49. Port Utilization Screen .....	78
Figure 6- 50. Port Error Statistic Screen .....	79
Figure 6- 51. Packet Analysis Table .....	79
Figure 6- 52. Browse Address Table Screen.....	80
Figure 6- 53. Switch History Screen .....	80
Figure 6- 54. Switch Utilities Menu.....	81
Figure 6- 55. Upgrade Firmware Screen.....	81



---

Figure 6- 56. Use Configuration File on TFTP Server Screen.....	82
Figure 6- 57. Save Settings to TFTP Server Screen.....	83
Figure 6- 58. Save Log to TFTP Server Screen .....	83
Figure 6- 59. Ping Test Screen.....	84
Figure 6- 60. Local Loopback Test Screen .....	84
Figure 6- 61. Line Loopback Test Screen.....	85
Figure 6- 62. System Reboot menu.....	86
Figure 6- 63. System Reboot Confirmation Screen .....	87
<b>Web-based Configuration</b>	
Figure7- 1. Web Manager Login.....	89
Figure7- 2. Top Section of Web Manager.....	89
Figure7- 3. Web Manager Folders and Menus.....	90
Figure7- 4. First Menu – System Information.....	91
Figure7- 5. Setup System Time Menu .....	91
Figure7- 6. IP Settings Window.....	92
Figure7- 7. Switch Information.....	92
Figure7- 8. Stacking Configuration Menu .....	93
Figure7- 9. Configure Port Table .....	94
Figure7- 10. Configure Port Settings Window.....	95
Figure7- 11. Configure Slot Module Port Window.....	95
Figure7- 12. Configure Port Security Window .....	96
Figure7- 13. Configure Individual Port Security Menu .....	97
Figure7- 14. 802.1X Capability Settings window .....	98
Figure7- 15. Initialize Port window .....	99
Figure7- 16. Reauthenticate Port window.....	99
Figure7- 17. 802.1X Authenticator Settings window.....	100
Figure7- 18. General Radius Server Setting window.....	102
Figure7- 19. Authentic Radius Server Setting window.....	103
Figure7- 20. Local Users Setting window.....	104
Figure7- 21. Port Mirroring window.....	104
Figure7- 22. Switch Settings.....	105
Figure7- 23. VDSL Settings Menu .....	106
Figure7- 24. 802.1Q Static VLANs Screen.....	107
Figure7- 25. 802.1Q Static VLANs Entry Settings – Add Screen .....	107
Figure7- 26. 802.1Q Static VLANs Entry Settings – Edit Screen .....	108
Figure7- 27. Port VLAN ID (PVID) Screen .....	109
Figure7- 28. Port Ingress Filter Screen .....	110

---

Figure7- 29. Configure Asymmetric VLANs Menu .....	111
Figure7- 30. Group Address Filtering Menu.....	111
Figure7- 31. Setup IEEE 802.1Q Multicast Forwarding Screen .....	112
Figure7- 32. IGMP Snooping Settings Screen .....	112
Figure7- 33. Setup Port Priority .....	114
Figure7- 34. STP Switch Settings Menu .....	115
Figure7- 35. Spanning Tree Port Settings .....	116
Figure7- 36. MAC Address Forwarding Entry Screen.....	117
Figure7- 37. MAC Address Filtering Setup Screen .....	117
Figure7- 38. Management Station IP Address Screen .....	118
Figure7- 39. Community Strings Menu .....	118
Figure7- 40. Trap Receivers Menu .....	119
Figure7- 41. User Accounts Control Table .....	119
Figure7- 42. Add User Accounts Control Table .....	120
Figure7- 43. Edit User Accounts Table.....	120
Figure7- 44. Serial Port Settings .....	121
Figure7- 45. Utilization window .....	123
Figure7- 46. Rx Packets Analysis window (Line Chart).....	124
Figure7- 47. Rx Packets Analysis window (Table).....	124
Figure7- 48. Rx Packets Analysis window for UMB (Line Chart).....	125
Figure7- 49. Rx Packets Analysis window for MBU (Table).....	126
Figure7- 50. Tx Packets Analysis window (Line Chart).....	127
Figure7- 51. Tx Packets Analysis window (Table).....	127
Figure7- 52. Rx Error Analysis window (Line Chart) .....	128
Figure7- 53. Rx Error Analysis window (Table) .....	129
Figure7- 54. Tx Error Analysis window (Line Chart).....	130
Figure7- 55. Tx Error Analysis window (Table).....	130
Figure7- 56. Tx/Rx Size Analysis window (Line Chart) .....	131
Figure7- 57. Packet Analysis window (Table).....	132
Figure7- 58. MAC Address Table window .....	133
Figure7- 59. IGMP Snooping Table window .....	134
Figure7- 60. Authenticator Status window .....	135
Figure7- 61. Authenticator Statistics window .....	135
Figure7- 62. Authenticator Session Counter window .....	136
Figure7- 63. Show Radius Authentication window .....	136
Figure7- 64. Show Radius Accounting window .....	137
Figure7- 65. Update Firmware from Server window .....	138

---

Figure7- 66. Use Configuration File on Server window .....	138
Figure7- 67. Save Settings To TFTP Server window .....	139
Figure7- 68. Save Switch History To TFTP Server window .....	139
Figure7- 69. Switch History window .....	140
Figure7- 70. Ping Test window .....	141
Figure7- 71. Local Loopback Test Screen .....	141
Figure7- 72. Line Loopback Test Screen .....	142
Figure7- 73. Save Configuration window .....	142
Figure7- 74. Factory Reset to Default Value window.....	142
Figure7- 75. Restart System window .....	143



# About This Guide

This User's guide tells you how to install, manage and configure the D-LINK DHS-3224V Switch.

## Overview of this User's Guide

- “*Introduction.*” Describes the Switch and its features.
- “*Installation and Setup.*” Discusses physical installation of the DHS-3224V Switch and SP-24 DSL Splitter.
- “*Switch Components.*” Describes the front panel, rear panel, and LED indicators of the Switch.
- “*Network Connections.*” Tells how you can connect the Switch and DSL Splitter to create a VDSL local area network (LAN).
- “*Switch Management Concepts.*” Explains some of the basic principles and concepts of Ethernet standards.
- “*Configuring the Switch.*” Tells how to use the built-in console interface to change, set, and monitor Switch performance and security.
- Appendix A, “*Technical Specifications.*” Lists the technical specifications of the DHS-3224V and the SP-24.
- Appendix B, Default Runtime Settings

## Intended Audience

It is assumed by the author that the reader of this user's guide has a basic understanding of the data packet switching and telecommunications technology in general, and its associated vocabulary. Some readers may not be familiar with Ethernet and the principles fundamental to Ethernet packet switching. For this reason, a discussion of the Ethernet concepts pertinent to the management of a Layer 2 Ethernet switch are provided in Chapter 5.

## Terminology

For convenience, the term Switch with an upper case “S” is used when specifically referring to the D-LINK DHS-3224V Switch. The term switch with a lower case “s” is a general term referring to all Ethernet-based switches. Likewise, the term Splitter or DSL Splitter is used to specifically refer to the D-LINK SP-24 DSL Splitter.



## Introduction

This section introduces the DHS-3224V VDSL Switch and describes essential functions and features of the Switch. A brief description of the system and its functionality are also presented.

### Ethernet over VDSL

The DHS-3224V Switch is used in concert with the SP-24 DSL Splitter and the CPE (DEV-301, DEV-304) to provide high-speed Internet connectivity to VDSL subscribers while maintaining full support for traditional analog voice telephone services. The Switch implements Ethernet over VDSL using existing twisted-pair copper telephone cable.

### Applications

Ethernet over VDSL systems are ideally suited for delivery of fast network services to dwellings and businesses with a high concentration of subscribers. Typical applications would include:

- Multiple Tenant Units (MTU) such as hotels
- Multiple Dwelling Units (MDU) such as high-rise apartment buildings
- Campus Networking
- LAN Extensions

Figure 1-1 below is a general representation of the D-LINK Ethernet over VDSL solution.

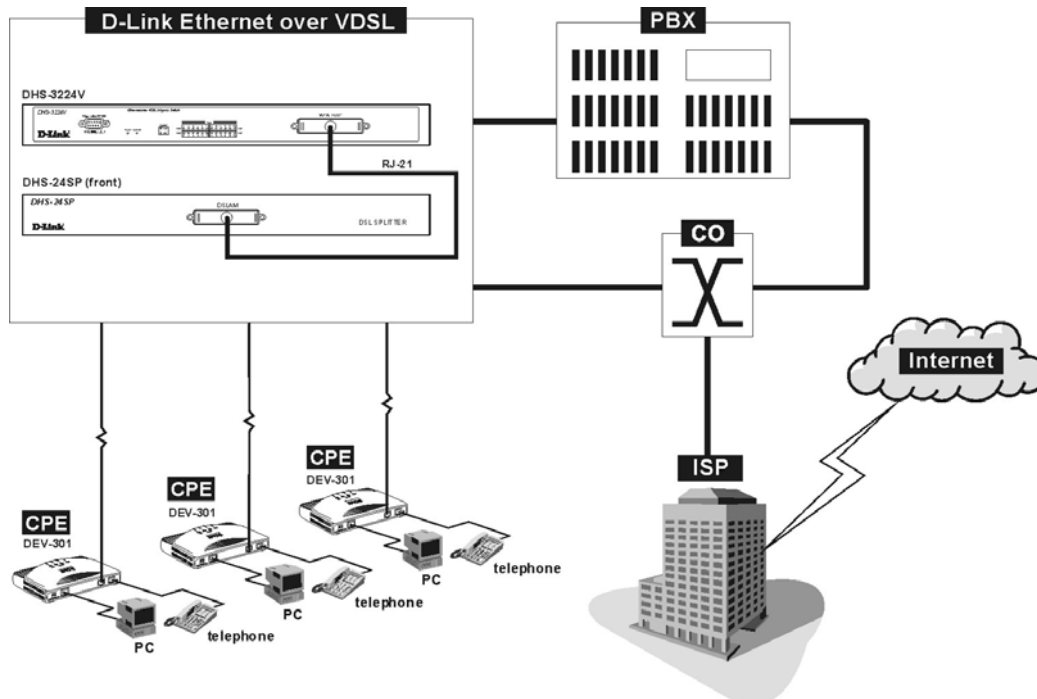


Figure 1-1. Ethernet over VDSL

## **Hardware**

The hardware components that comprise the D-LINK Ethernet over VDSL solution include the following:

1. The D-LINK DHS-3224V 24-port VDSL Switch
2. The D-LINK SP-24 DSL Splitter. Each unit channels voice and data to up to 24 end users, therefore, one DSL Splitter must be installed for every Switch.
3. The D-LINK DEV-301 and DEV-304 used to connect end users to both data and voice channels. These VDSL Bridges separates the lower frequency analog voice services from the high-speed digital data channel and delivers both on separate lines..

The Switch and DSL Splitter function to concentrate and manage end user network connections and multiplex voice telephony and data services. The Switch/Splitter combination is in effect the DSLAM for the local VDSL subscribers.



---

## Switch Description and Function

---

The DHS-3224V VDSL Switch is an Ethernet-based switch capable of delivering VDSL service via installed telephone cabling. Up to 24 VDSL accounts can be managed per Switch and up to 6 Switches can be set up in a stacked group configuration. Each Switch paired with an on-site SP-24 DSL Splitter and remote CPE (1 unit per port). The splitter combines the VDSL data channels and lower frequency analog telephone services (including ISDN) and transmits the combined services to the end-users. For the VDSL subscriber, the CPE separates the data and voice channels with a built-in splitter allowing simultaneous, full-duplex VDSL and analog voice transmission. In this way, Ethernet over VDSL can overlay existing service without additional cable installation or conditioning.

The Switch functions as a conventional Ethernet switch where each port provides VDSL service to a single account. The local Ethernet-based network however, differs from standard Ethernet in two significant ways:

**Cabling** – The Switch provides VDSL service via existing 0.4 mm or 0.5 mm twisted-pair telephone cable.

**Reach** – VDSL service from the Switch to the subscriber can extend far beyond the maximum reach of standard Ethernet.

The Switch can be managed via an out-of-band console connection to a computer using terminal emulation software. The manager console may also be accessed in-band using an SNMP network manager or Telnet. Management functions will be familiar to users who have worked with Layer 2 Ethernet switches. For users not familiar with Ethernet switches and switch management, a detailed explanation of some of the important management concepts and Ethernet standards is provided in Chapter 5.

## Features

---

### Ports

- One female RJ-21 port for connection to a VDSL splitter using Telco50 cabling.
- Uplink module with one 10/100 BASE-TX port for Ethernet over VDSL Uplink.
- 2 x IEEE1394 (Rx + Tx) "FireWire" ports for Switch-to-Switch operations.
- One female 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

- Quadrature Amplitude Modulation (QAM)
- Frequency Division Duplexing
- Spectral compatibility with xDSL, ISDN (2B1Q/4B3T), digital PBX extensions and narrow band interference
- 8.8 Gbps switching fabric capacity
- Store and forward switching scheme.
- 8K active MAC address entry table per device with automatic learning and aging (10 to 1000000 seconds).
- 8 MB packet buffer per device.
- 802.1D Spanning Tree support.
- 802.1Q Tagged VLAN support
- Supports up to 24 end users per Switch (24 ports)
- Up to 6 Switches can be stacked in a 19" equipment rack and managed as a unit

### Management

- Provisioning for VDSL Settings (per Port)
- RS-232 console port for out-of-band network management via a console terminal.
- Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops.
- SNMP v.1 Agent.
- 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.
- Built-in SNMP management:
  - Bridge MIB (RFC 1493)
  - MIB-II (RFC 1213)
  - Mini-RMON MIB (RFC 1757) – 4 groups
  - 802.1p MIB (RFC 2674).
- TFTP support
- BOOTP support
- DHCP Client support
- Password enabled.
- Telnet remote control console
- Web Management Software

# 2

## ***Installation and Setup***

Please read this section carefully to be certain that all equipment is installed and set up in accordance with the instructions given here.

### **Unpacking**

Each shipping carton should contain the following items:

- ✓ One DHS-3224V VDSL Switch
- ✓ Mounting kit: 2 mounting brackets and screws
- ✓ Four self-adhesive rubber feet
- ✓ One AC power cord
- ✓ This User's Guide

If any item is found missing or damaged, please contact your D-LINK representative or sales agent.

### **Switch Placement**

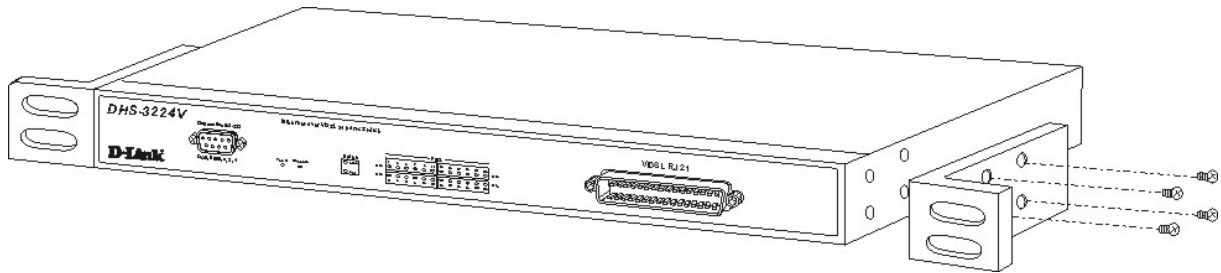
The Switch and Splitter are designed for mounting in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. Make certain the location of the equipment rack is sufficiently dry and cool. See the Specifications in Appendix A for environmental requirements and limitations. Use these additional guidelines when selecting a suitable location for the equipment rack.

- ➔ Attach the rubber feet to all Switches and Splitters that will be installed to maintain a minimum space between the devices and to avoid damaging the equipment housing.
- ➔ If you are installing more than one Switch, read *Connecting Multiple Switches* in Chapter 4.
- ➔ 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 and Splitter. Leave at least 5cm of space on the right and left sides, as well as 5cm on the rear of the equipment for ventilation.
- ➔ Cables for both devices attach at the front and the rear. Make sure there is ample room at the front and the back of the devices to access cable connections.
- ➔ Do not place heavy objects on the Switch or Splitter.

## Rack Installation

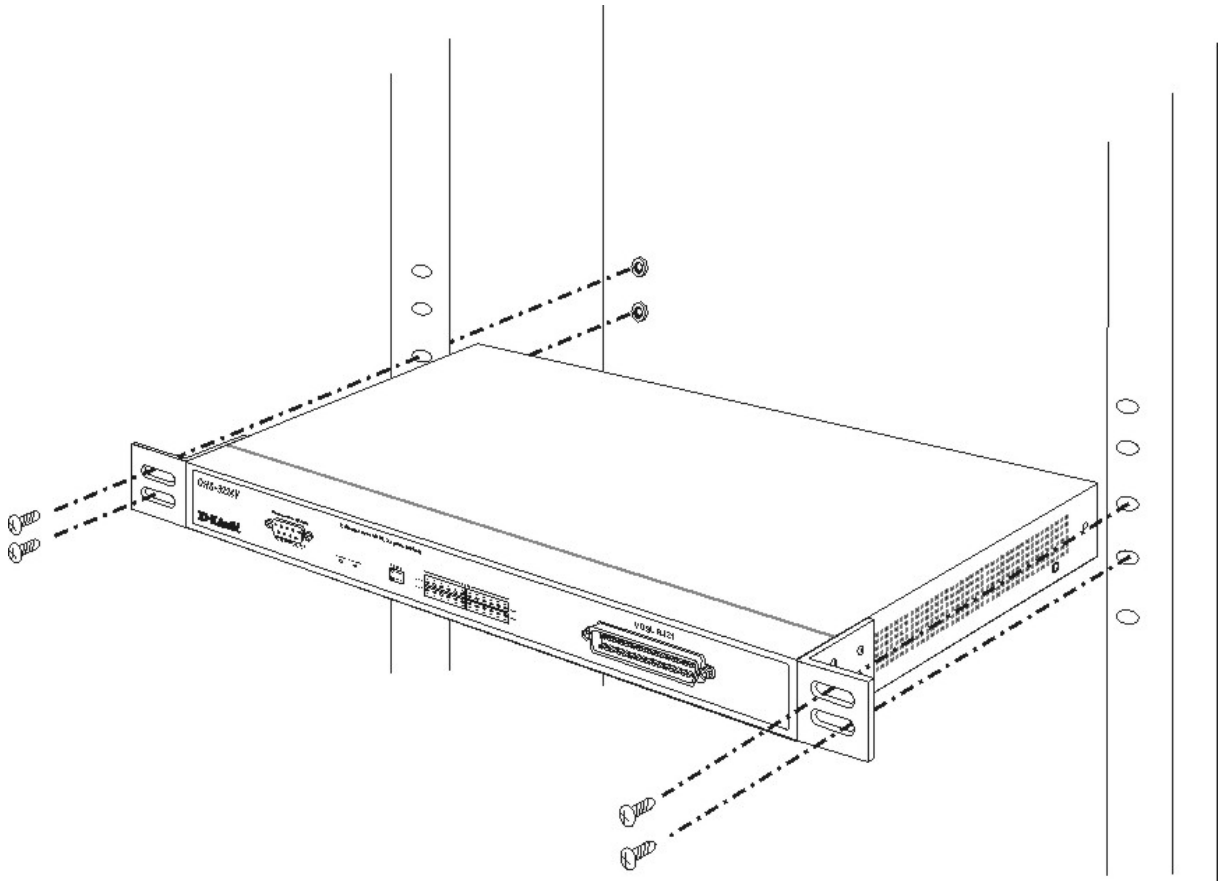
**IMPORTANT:** Attach the included rubber feet to the Switch or Switches before installing it in the rack. All equipment in the rack including DSL Splitters should have rubber feet attached. This is to maintain the minimum space needed between the devices and to protect the device housing from being damaged.

Use the diagrams below as a guide for mounting both the Switch and SP-24 Splitter.



**Figure 2-1. Attaching the mounting brackets to the Switch**

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



**Figure 2-2. 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. It may be powered on without having any or all network cables connected.

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

- The console LED indicator will blink green. This blinking of the LED indicators represents a reset of the system.
- The power LED indicator will light steady green

## **Power Failure**

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

## 3

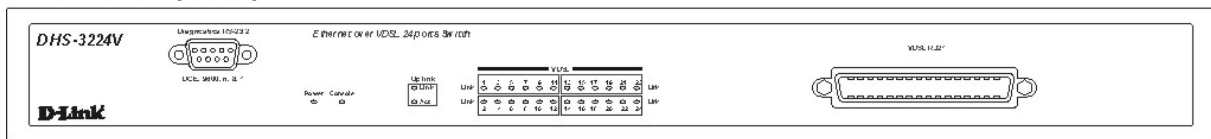
## Switch Components

This chapter describes the front panel, rear panel, side panels, optional plug-in modules, and LED indicators of the DHS-3224V.

### Front Panel

The front panel of the Switch consists of LED indicators, an RS-232 communication port, and an RJ-21 port for connection to the SPT48JA Splitter.

#### DHS-3224V (front)

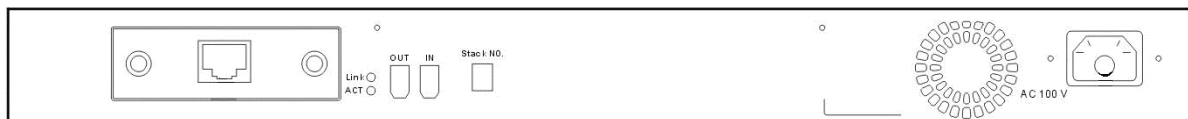


**Figure 3-1. Front panel view of the Switch**

- Comprehensive LED indicators display the status of the Switch and the network (see the *LED Indicators* section below).
- An RS-232 DCE console port for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.
- A VDSL RJ-21 port for connection to a DSL Splitter (SP-24)

### Rear Panel

The rear panel of the Switch contains an AC power connector and the VDSL Uplink module.

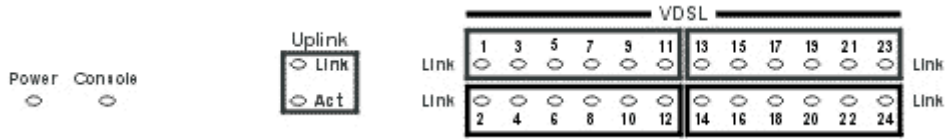


**Figure 3-2. Rear panel view of the Switch**

- The AC power connector is a standard three-pronged connector that supports the power cord.
- 10/100 BASE-TX module used for uplinking to the Ethernet backbone.

## 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 3-3. The LED indicators**

- **Power:** This indicator lights steady green when Switch is powered on and is dark when there is no power supplied.
- **Console:** This indicator lights steady 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. It will blink during the power on (POST) initialization.
- **Uplink Link:** This indicator (located on the rear panel next to the Uplink port) will light green when a valid link to Ethernet (network backbone) is established. It will be dark if there is no link.
- **Uplink Act:** This indicator (located on the rear panel next to the Uplink port) will blink green when there is activity, data transmission or reception, on the Uplink to the Ethernet (network backbone).
- **VDSL Link:** This indicator will light green when a valid VDSL link is established. It will be dark if there is no link.

## Network Connections

This chapter describes how to connect the Switch as a standalone device or in a group to one or more SP-24 Switches. The Switch provides the Ethernet over VDSL Uplink to the central office while the splitter combines the VDSL data channel and basic telephone services for transport to end users.

Network cable connections can be made to the Switch with the power on or off. Caution should always be used when working with or handling any electrically powered devices.

The cable connections described in detail in this chapter include:

### Connections to the Switch

- Switch-to-Switch connection via IEEE 1394 "FireWire" for multiple Switch installation
- Switch to backbone; (VDSL over Ethernet) Uplink to backbone via RJ-45 Ethernet port
- Switch to SP-24DSL Splitter via Telco50 cable (RJ-21 port)

### Connections to SP-24DSL Splitter

- Splitter to Switch or Switch pair via Telco50 (RJ-21 connector) cable
- Splitter to CPE (via 0.4mm or 0.5mm twisted-pair telephone cabling)
- Splitter to PBX (analog channel to Central Office) for basic telephone services

The Switch-to-computer connection via the RS-232 port (used for device/network management) is discussed in Chapter 5.

The devices described here are designed for installation in a standard 19" rack where cable connections can be easily accessed from both the front and the rear of the rack. Please read Chapter 2 for information about how to install the devices in an equipment rack. The cable connections are described in two sections, one for connections made using the ports on the front of the equipment and another for the connections made on the back.

## Connecting Multiple Switches

Up to 6 Switches may be grouped in a stacked configuration and connected together using FireWire cabling. A multiple Switch arrangement can be connected to share a single uplink to the Ethernet backbone and be placed in a single 19" equipment rack. Stacked switch group interconnections use IEEE 1394 FireWire.

**Note:** IEEE 1394 "FireWire" is a serial bus technology defined by the IEEE1394 High Performance Serial Bus standard. For information about IEEE 1394, go to the 1394 Trade Association web site: <http://www.1394ta>.

## Stacking a Switch Group

Up to 6 Switches may be stacked and managed as a unit with a single IP address and single uplink to the Ethernet backbone. If you use the stacking function, it is important that you understand how stacking works in the Switch, read Managing Switch Stacks and Determining Stack Order in Chapter 5 before placing the Switches in the rack. The auto-detect feature for establishing the stack hierarchy can be overridden, see Stacking Configuration in Chapter 6 for details on changing the stack order.

Figure 4-2 below illustrates how the Switch stack should be connected.



## **Powering On Switch Stacks**

Switches in stacked Switch groups should be powered on simultaneously after all the FireWire connections are in place. The auto-detect mechanism of the stacking function requires that all participating Switches share MAC address information at the same time to establish the stack order. Once the group hierarchy has been established, it can only be changed using a software-driven override or a factory reset of each Switch in the group followed by simultaneous power on.

## **Cable Connections for a Stacked Switch Group**

Interconnection of the Switch stack is accomplished using IEEE 1394 "FireWire" cabling. The ports used to connect the Switch stack are referred to here as the "stacking" ports. For uplink to the Ethernet backbone, it is recommended that the Master Switch be used, although other Switches in the stack can be used for uplink. Follow these steps to connect the stacked devices:

1. Connect the FireWire port on the Master Switch labeled "Out" to the FireWire port labeled "In" on the Number 2 Switch.
2. Connect the FireWire port of the Number 2 Switch labeled "Out" to the FireWire port of the Number 3 Switch. Continue to connect the stacking ports of all the Switches in the stack in a likewise fashion.
3. Connect the FireWire port labeled "Out" on the last Switch in the stack i.e. the highest numbered Switch, to the FireWire port labeled "In" on the Master Switch.
4. Finally, you can connect the Uplink port (10/100BASE-TX) to the Ethernet backbone with Category 5 cabling with RJ-45 connectors.

Figure 4-1. Switch Stack Connections below illustrates cabling for a stacked group of six DHS-3224V Switches.

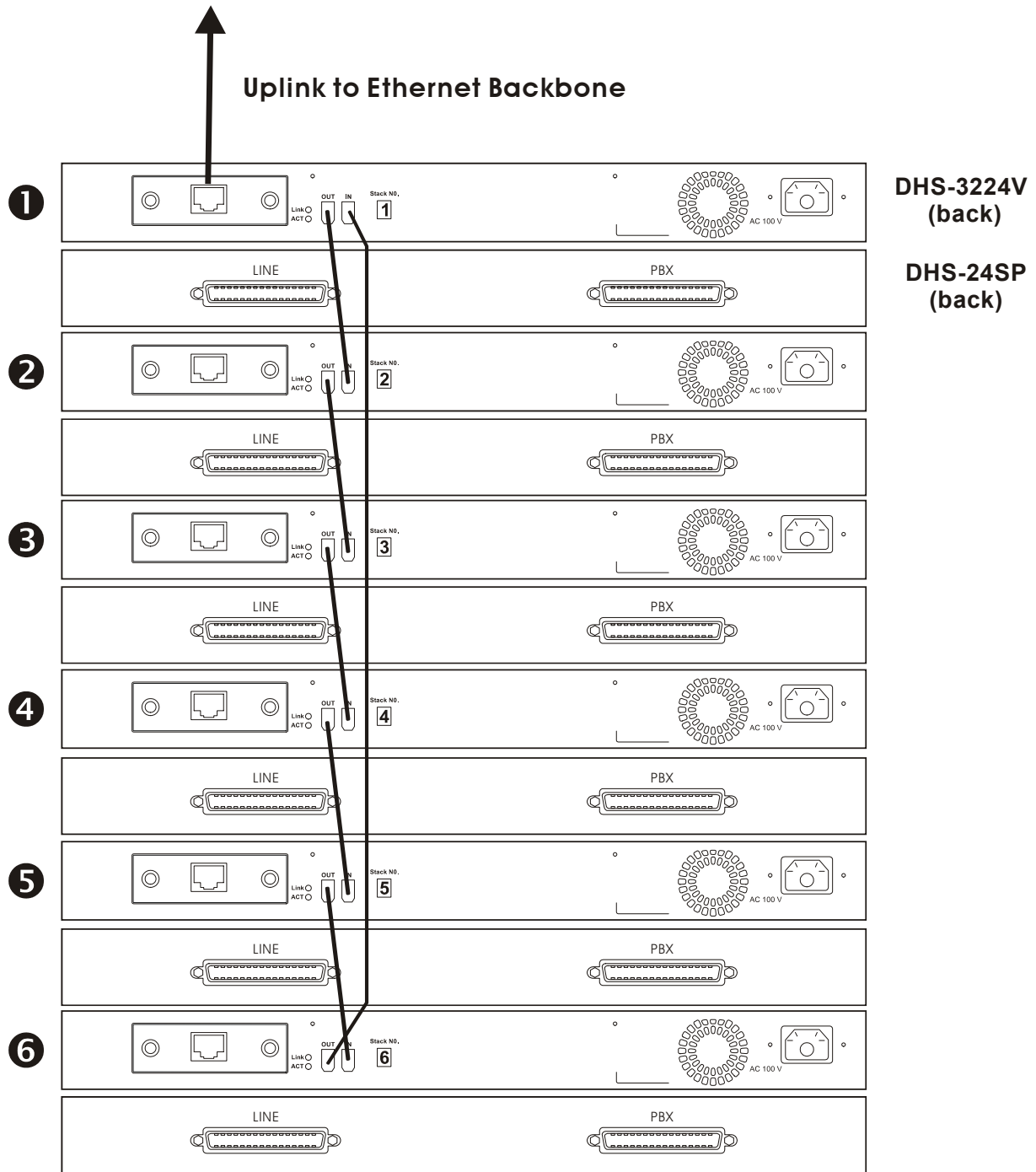


Figure 4-1. Switch Stack Connections

## Front Panel Connections

The front view of the Switch and VDSL Splitter are illustrated in the diagram below. Three connections are required:

1. Connect the female RJ-21 receptacle (labeled *DSLAM*) on the SP-24 DSL Splitter to the female RJ-21 receptacle (labeled *VDSL RJ-21*) on the front panel of the DHS-3224V Switch with Telco50 cable with RJ-21 connectors (male-to-male).
2. If you are connecting a second Switch to the Splitter, connect the remaining female RJ-21 receptacle (labeled *DSLAM*) on the SP-24 DSL Splitter to the female RJ-21 receptacle (labeled *VDSL RJ-21*) on the front panel of the DHS-3224V Switch with Telco50 cabling with RJ-21 connectors (male-to-male).
3. For initial set up and management, connect the male RS-232 port on the Master Switch to the computer used for Switch configuration and management using RS-232 cable.

### DHS-3224V

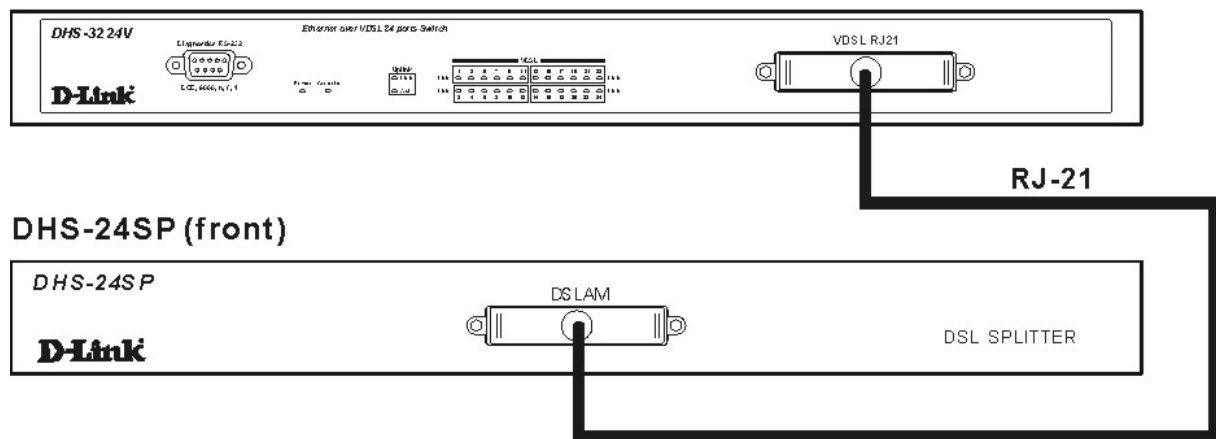


Figure 4-2. Front Panel Network Connections

## Rear Panel Connections

The rear panel connections of the DHS-3224V Switch and SP-24 Splitter are illustrated in the diagram below. The necessary connections are:

1. Connect the female RJ-21 interface (labeled *PSTN A* or *PSTN B*) on the rear panel of the SP-24 DSL Splitter to the PBX (POTS line) using RJ-21 cable.
2. Connect the female RJ-21 interface (labeled *LINE A* or *LINE B*) on the rear panel of the Splitter to the Main Distribution Frame, Cabling Cabinet or other wiring system used for connection the end users. This connection is made using Telco50 cable with a male RJ-21 connector.
3. Connect the 10/100BASE-TX Uplink port to the Ethernet backbone using Category 5 or better twisted-pair cabling with RJ-45 connector.

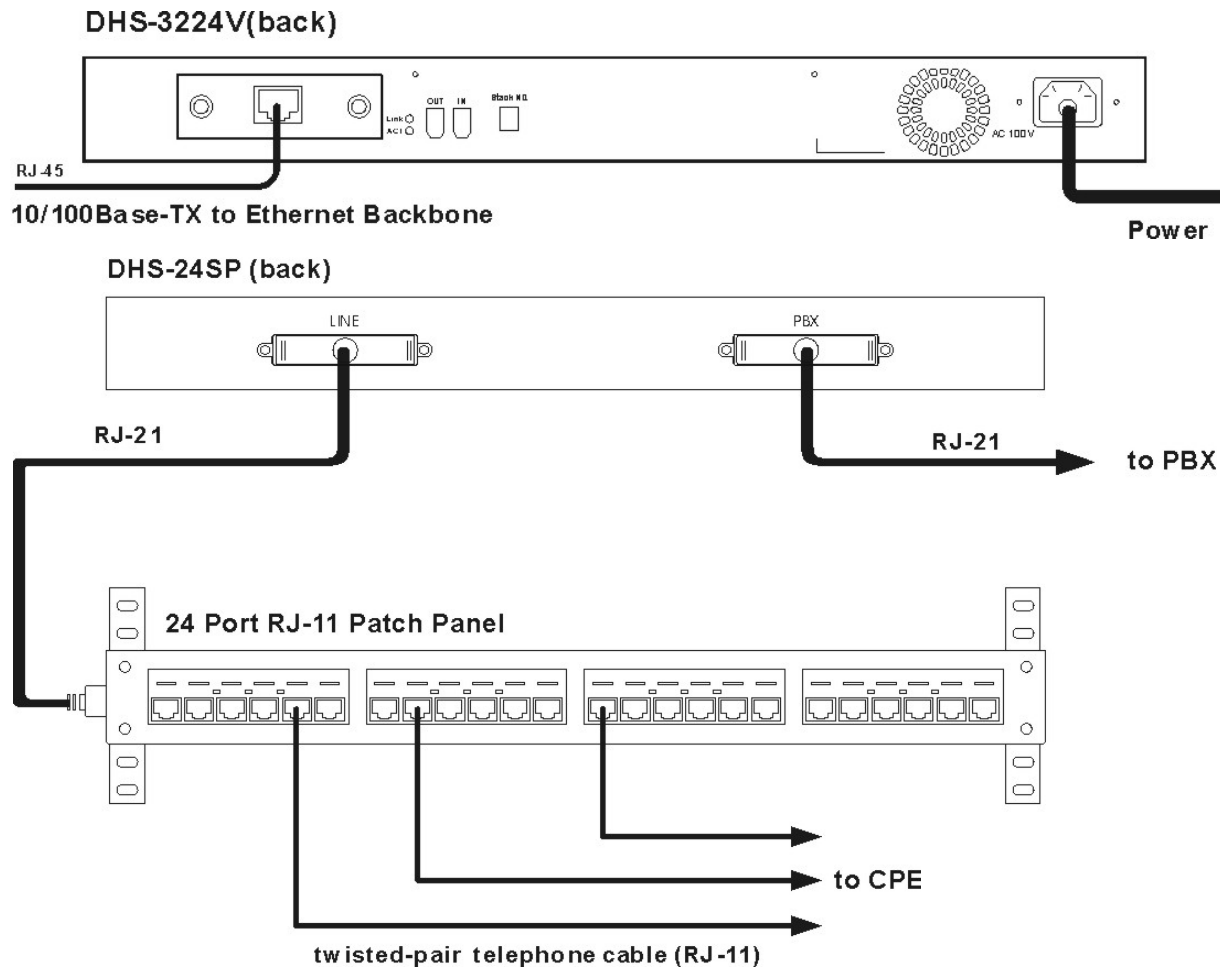


Figure 4-3. Rear Panel Connections

**Note:** In Figure 4-3. Rear Panel Connections, a 24-port RJ-11 patch panel is used for the purpose of illustrating the Splitter-to-subscriber connection.

## Network Connections to DSL Splitter

The SP-24 DSL Splitter connects VDSL subscribers to both voice and data channels. All interfaces on the DSL Splitter are female RJ-21 ports. All connection to the DSL Splitter should be made using Telco50 cabling with male RJ-21 connectors. The DSL Splitter may be connected or disconnected while the Switch is powered on or off. Figure 4-4 below illustrates the connection to the DSL Splitter.

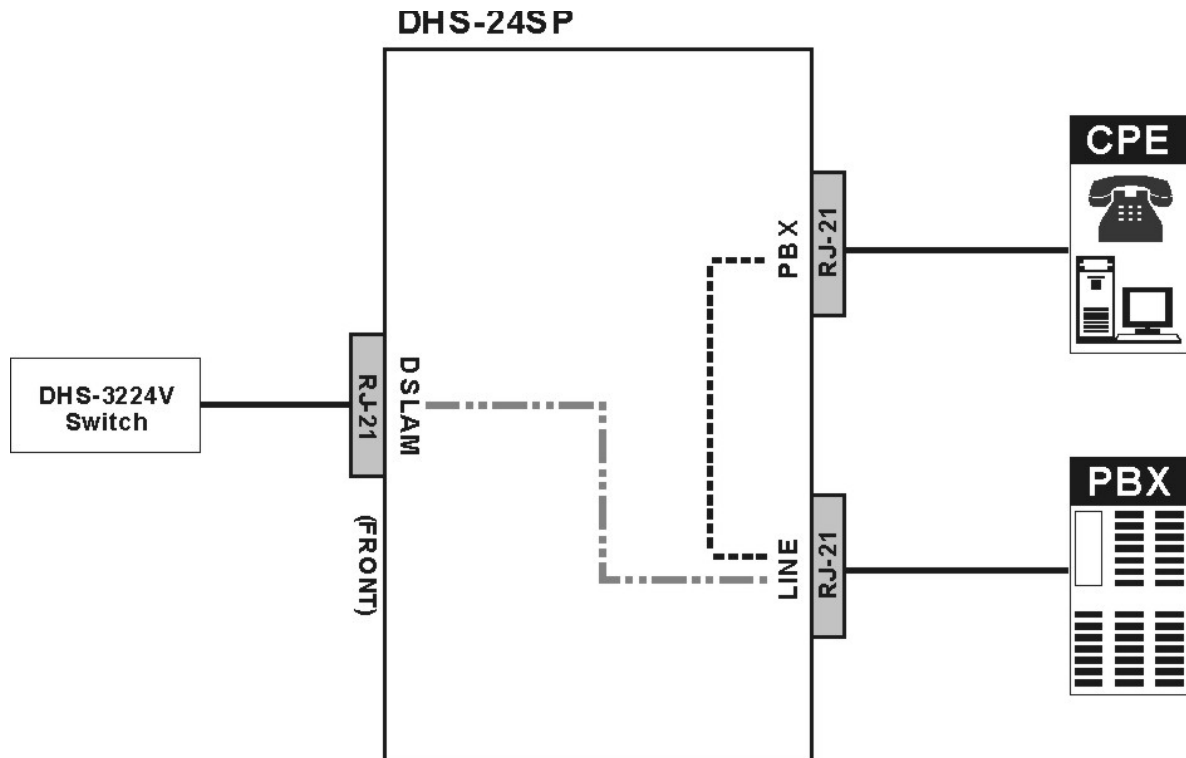


Figure 4-4. Connection to the DSL Splitter

Connect the SP-24 DSL Splitter as follows:

1. Connection(s) to the DHS-3224V Switch are made via the RJ-21 port on the front panel of the device labeled *DSLAM*. The Splitter is connected to one VDSL Switch. Connection to the Switch provides the VDSL data channel (over Ethernet) to end users. Up to 24 VDSL accounts may be connected through each DSLAM port (24 VDSL subscribers per DSL Splitter).
2. Connection(s) to the PBX are made via the RJ-21 ports labeled *PBX*. This connects the DSL Splitter to the PBX and provides the channel for analog voice services.
3. Connections to the remote up to 24 CPE are made by first connecting to a Main Distribution Frame, Cabling Cabinet, patch panels or other suitable wiring systems. Use the RJ-21 ports labeled *LINE* to connect the combined data and voice channels to the VDSL accounts.

## Cable Attachments to DSL Splitter

There are two styles of connectors used for RJ-21 cable connections. The recommended style for all RJ-21 connections on the Switch and Splitter is the 90-degree connector picture in Figure 4-5 below.

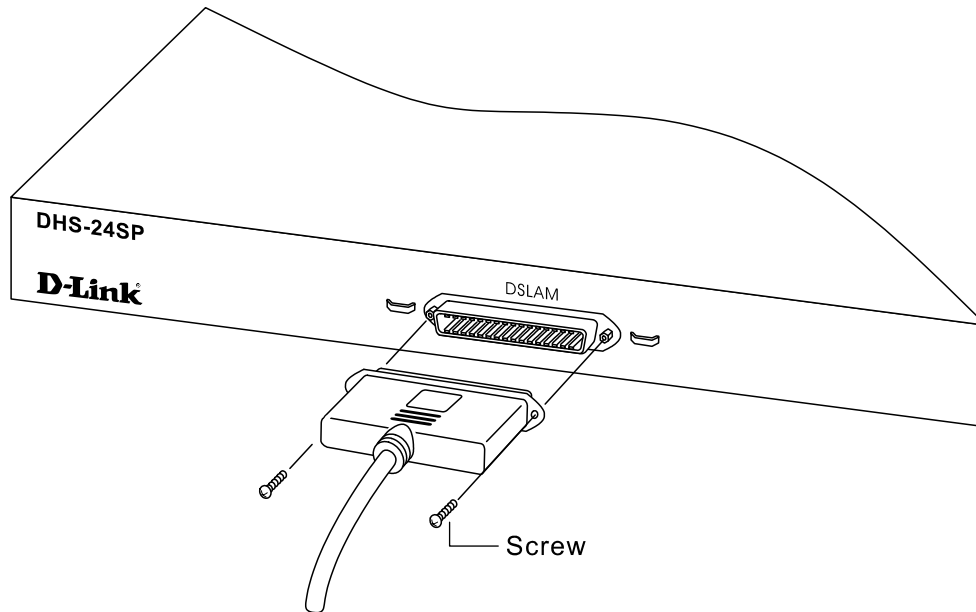


Figure 4-5. 90-degree Connector secured with two screws

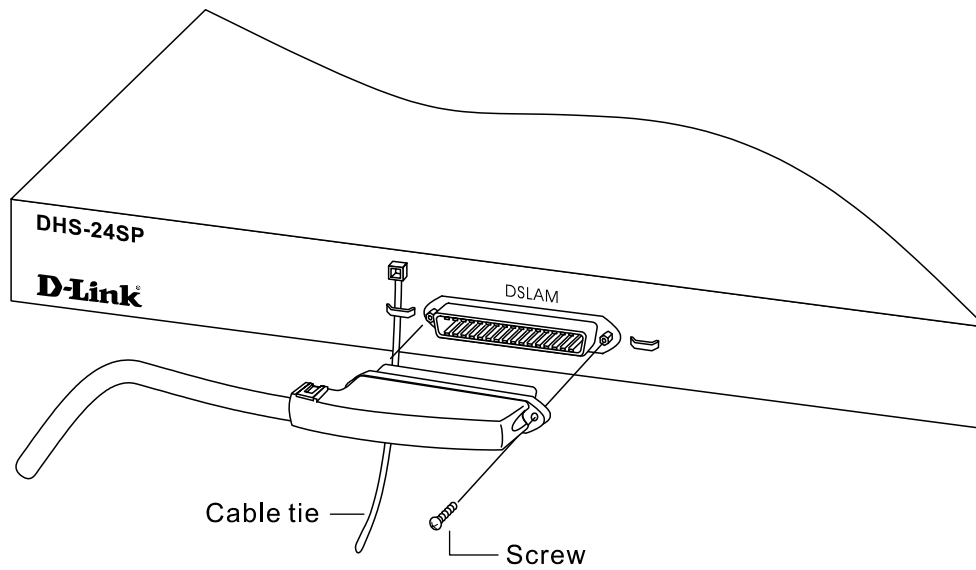


Figure 4-6. 120-degree Connector secured with one screw and a cable tie

## Install the Ground Wire on the DSL Splitter

The DSL Splitter chassis must be properly grounded. A ground connection for this purpose is located on the front panel of the Splitter (near the D-LINK logo). Use 10 – 12 gauge (or heavier) copper wire for grounding the Splitter. Attach the ground wire securely to a suitable grounding post. See Figure 4-7 below.

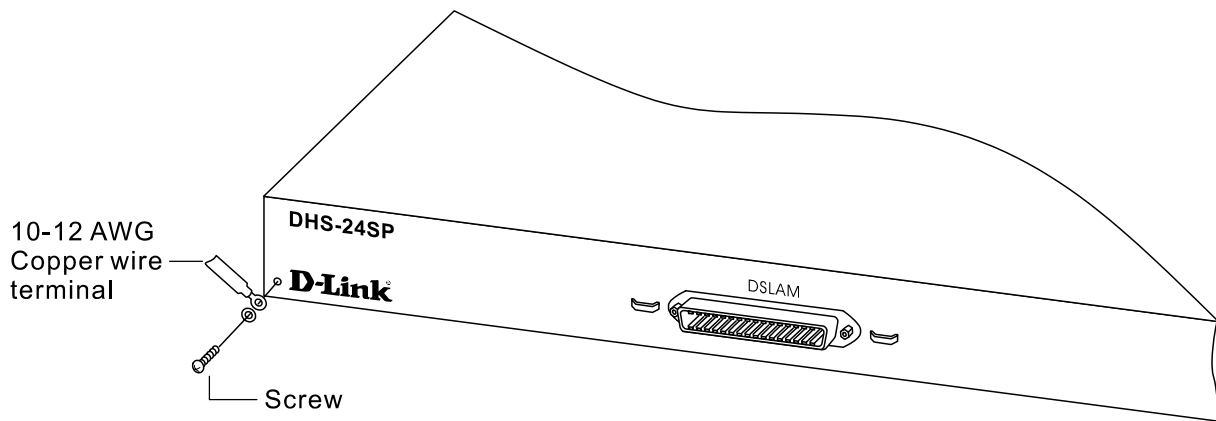


Figure 4-6. Ground Wire for DSL Splitter

## Connection to End User

The separate signals for both VDSL and POTS service are carried to subscribers via standard 0.4mm or 0.5mm twisted-pair telephone cabling. Connection to the CPE is made with standard RJ-11 connectors that are familiar to the subscriber. The CPE device is a simple bridge and does not require that any driver or software be installed by the subscriber. Therefore, remote installation of CPE should not be difficult.

When the Ethernet over VDSL System has been connected, service must be enabled for each connected port. It may also be necessary to change the connection speed for the individual ports. Ports on the Switch are enabled and configured using the Configure Ports option of the console manager. See the Configure Ports section in Chapter 6 for information on enabling port and controlling port bit rates.

## Switch Management Concepts

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

- **Local Console Management**
- **IP Addresses and SNMP Community Names**
- **Traps**
- **MIBs**
- **Packet Forwarding**
- **SNMP**
- **Spanning Tree Protocol**
- **VLANs**

### 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.

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

The DHS-3224V Switch 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 (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 to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called Local Console Management to differentiate it from management done via management platforms, such as HP OpenView.

The console port is set for the following configuration:

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

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

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try typing 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.

### Boot Screen

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. You will also find the MAC address printed on the rear panel of the device.

```
Boot Procedure                                     PROM Version: 1.00-B02
-----
Power On Self Test ..... 100 %
MAC Address   : 00-80-C8-E5-0E-22
H/W Version  : 2A1
Please wait, loading Runtime image ..... 100 %
```

Figure 5-1. Boot Screen

### Switch Information Screen

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

```
Switch Information
-----
Unit : <fl>
MAC Address       : 00-80-C8-E5-0E-22
Ext.Module Type  : 10/100 TX 1 Port Module
Ext.Module Version : 1A1
VDSL Patch File Version : 0x0058
Fan Status       : Good

*****
Function:Select the device.
Message:
CTRL+T = Root screen      Esc=Prev. screen      CTRL+R = Refresh
```

Figure 5-2. Switch Information Screen

## Remote Management Setup Menu

Use the Remote Management Setup menu to assign IP settings and SNMP assignments for the Switch. You can also set an IP Address for a gateway device such as a router or Layer 3 switch. 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 manager stations allowed 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 such as 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 monitor the state of devices in 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. Trap recipients are configured using the Remote Management Setup menu.

```

Remote Management Setup
-----
Current Switch IP Settings:           Management Station IP Settings:
Get IP From:      Manual              IP Address:[0.0.0.0      ]
IP Address:      10.90.90.90          IP Address:[0.0.0.0      ]
Subnet Mask:     255.0.0.0           IP Address:[0.0.0.0      ]
Default Gateway: 0.0.0.0
Management VID:  1

New Switch IP Settings:              SNMP Community Settings:
Get IP From:      <Manual>            Community String Rights  Status
IP Address:      [10.90.90.90 ]      [public      ]<Read> <Enabled >
Subnet Mask:     [255.0.0.0  ]      [private     ]<R/W > <Enabled >
Default Gateway: [0.0.0.0    ]      [            ]<Read> <Disabled>
Management VID:  [1          ]      [            ]<Read> <Disabled>

                                SETUP TRAP RECEIVERS    APPLY

*****
Function:Get IP from Manual, BOOTP or DHCP.
Message:
CTRL+T = Root screen      Esc=Prev. screen      CTRL+R = Refresh
    
```

Figure 5-3. Remote Management Setup

You can specify which network managers will 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 must be used by the management station software to access the switch.

The following are examples of trap types:

### Cold Start

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

### Authentication Failure

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

### **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 it is elected 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**

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.

### **Fan Failure**

A Fan Failure trap is sent if any of the four system fans fail.

### **Link Change Event**

**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.

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 the kilobytes of data 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 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.

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

## Authentication

The authentication protocol ensures that the remote user SNMP application program discards packets from unauthorized users. Authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application must use the community string. SNMP community strings of up to 20 characters may be entered under the Remote Management Setup menu of the console program.

## Packet Forwarding

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

## MAC Address Aging Time

The Aging Time affects the learning process of the Switch. Dynamic forwarding table entries are made up of the source and destination MAC addresses and their associated port numbers and 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.

## Packet 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 or an IP Address entered into the filter table, the switch will discard the packet.

Some filtering is done automatically by the switch:

Dynamic Filtering: automatic learning and aging of MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.

Filtering done by the Spanning Tree Protocol, which can filter packets based on topology, making sure that signal loops don't occur.

Filtering done for VLAN integrity. Packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3) will be filtered.

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

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

## Managing Switch Stacks

The Switch can be stacked in groups of up to six Switches. A Switch stack is managed as a single unit with a single IP address. The logical stack order is hardware-determined; the unique MAC address of each Switch determines their stack order. It is best to place stacked Switches in the equipment rack in their logical stack order when you first set them up. However, you can override the automatically determined stack order. For example, you may plan an expansion to the VDSL network and add another Switch. In this case, it may not be convenient to change the physical arrangement of the stack. You can override the normal order and force the group to use a logical stack arrangement that reflects the physical arrangement of the Switches. If you choose to employ Switch stacking, remember the following:

- Management of all the Switches in the stack is done through a master Switch.
- The master Switch should be used for the uplink to the Ethernet backbone.
- If any Switch in the stack fails, all Switches must be rebooted once the failure is corrected or the affected Switch is disabled.
- If a new master is elected, or if the stack order is changed, all Switches in the stack must be rebooted.
- The master Switch will be chosen automatically when the stack is powered on. The Switch with the lowest value MAC address is elected to function as the master. The remaining Switches are ordered according to the relative value of their respective MAC addresses (see the example below).
- For a first time set up of a stack group, power on all Switches simultaneously after the FireWire interconnections are completed (See Figure 4-1. Switch Stack Connections).
- The normal stack order determined by the Switch MAC addresses can be overridden to suit your preference. See Stacking Configuration in Chapter 6 for details.

## Determining Switch Stack Order

If you are using a stacked switch arrangement it is important to understand how Switch stack order is established. For illustration, we use an example of four DHS-3224V Switches connected in a stacked arrangement and booted up. We assume that the Switches are booted up simultaneously and initiate a discovery process to determine the logical stack order. The logical stack order is a function of MAC address as demonstrated below. Once the stack order has been determined, any additions to the stack will affect the stack order. In addition, the new stack order is a function of the MAC address AND the already established stack order. That is, the original stack order plays a role in any subsequent changes to the stack when the order is automatically determined. Auto-detect uses the following formula: **MAC Address + Stack Order #** to establish the stack order. When there is no established stack order, the stack order number = 0 in the formula. Using the auto-detect stacking function, the four MAC addresses are ordered as listed in Figure 5-4. Initial Stack Order below:

Stack Order	MAC Address	MAC + Stack #	Stack order after boot up
0	001122334451	<b>001122334451+0 = *51</b>	<b>1 (Master Switch)</b>
0	001122334452	001122334452+0 = *52	2
0	001122334453	001122334453+0 = *53	3
0	001122334454	001122334454+0 = *54	4
0	-	-	Not in use
0	-	-	Not in use

Figure 5-4. Initial Stack Order

Let us suppose you wish to add another Switch to the stack. The new Switch has a MAC address 001122334450. The new Switch is first inserted (logically) into the next available position in the stack, the number 5 position. Then the formula is applied to determine a new stack hierarchy. After rebooting all the Switches in the stack, the automatically determined stack order appears as listed in the Figure 5-5. New Stack Order below:

Original Stack Order	MAC Address	MAC + Stack #	New Stack Order
<b>1</b>	<b>001122334451</b>	<b>001122334451+1 = *52</b>	<b>1 (unchanged)</b>
2	001122334452	001122334452+2 = *54	2 (unchanged)
3	001122334453	001122334453+3 = *56	3 (new Switch)
4	001122334454	001122334454+4 = *58	4 (changed from position 3)
5 (new Switch)	001122334450	001122334450+5 = *55	5 (changed from position 4)
6	-	-	Not in use

Figure 5-5. New Stack Order

You can override the automatic stack order selection to place the newly added Switch into the number 5 position of the stack order (read *Error! Reference source not found.* in Chapter 6 for information on how to override the stack order auto-detect function).

**Note:** Remember that management of the Switch stack is done only through the Master Switch. Therefore if there is a new Master Switch after rebooting the new stack arrangement, it will be necessary to attach the serial cable to the new Master in order to override the auto-detect stack order or to make any configuration changes to any Switch in the stack.

## Spanning Tree Protocol

The IEEE 802.1D Spanning Tree Protocol (STP) 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 the duplicate links to be used in case 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 carefully read understand this section before making any changes from the default values.

The Switch allows two levels of spanning trees to be configured. The first level constructs a spanning tree among all links between network switches. This first level is referred to as the Switch or Global level. The second level is based on port groups. Groups of ports are configured as being members of a spanning tree and the algorithm and protocol are applied to the group of ports. This is referred to as the Port or VLAN level.

Spanning Tree on the Switch performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees - from any combination of ports contained within a single switch, in user-specified groups (usually VLANs).
- 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

STP operates on two levels: the switch level and the port or VLAN 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, then sets the root bridge and the designated bridges.

On the port level, STP sets the root port and designated ports.

## Switch Level STP

The switch STP parameters listed here can be configured by the user:

Parameter	Description	Default Value
<b>Bridge Identifier</b> (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
<b>Priority</b>	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
<b>Hello Time</b>	The length of time between broadcasts of the hello message by the switch	2 seconds
<b>Maximum Age Timer</b>	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
<b>Forward Delay Timer</b>	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

## Port Level STP

The VLAN or port STP parameters listed here may be configured by the user:

Variable	Description	Default Value
<b>Port Priority</b>	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
<b>Port Cost</b>	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path.	10 – 100Mbps Fast Ethernet ports

## Bridge Protocol Data Units

The Switch uses the following information for STP to stabilize network topology:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

This STP information is shared among 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 receive the BPDU. BPDUs are not directly forwarded by the switch, but 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.

## Transition States

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

Figure 5.4 below illustrates the STP port transition states.

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

### 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.

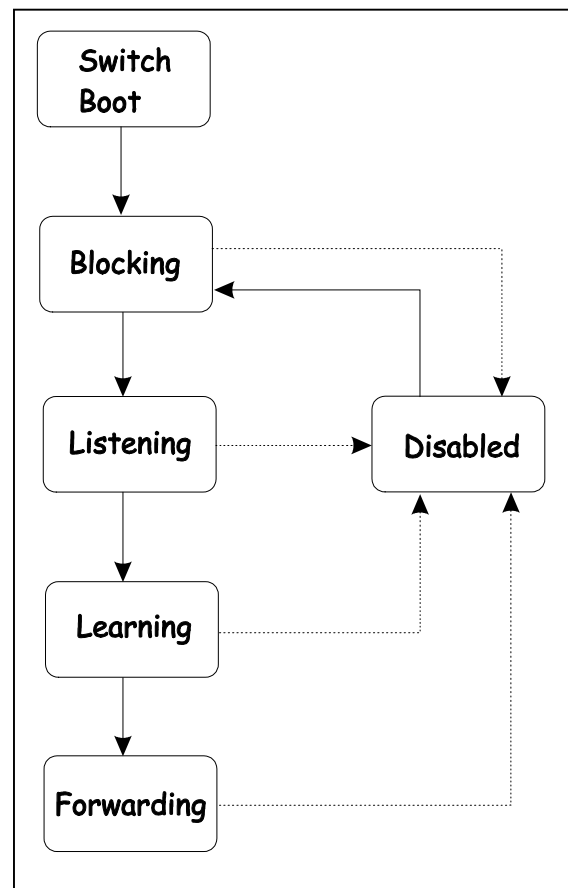


Figure 5-4. STP Transition States

### Port State Transition

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

The default Spanning Tree parameters are as follows:

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

## 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:

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

- **Max Age**

The Maximum Age Timer 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, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out the Switch has the lowest Bridge Identifier, it will become the Root Bridge.

- **Forward Delay**

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

- **Priority**

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

Observe the following formulas when setting the above parameters:

- Max. Age = 2 x (Forward Delay - 1 second)
- Max. Age = 2 x (Hello Time + 1 second)
- 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 5.5. 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 5.6. 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.

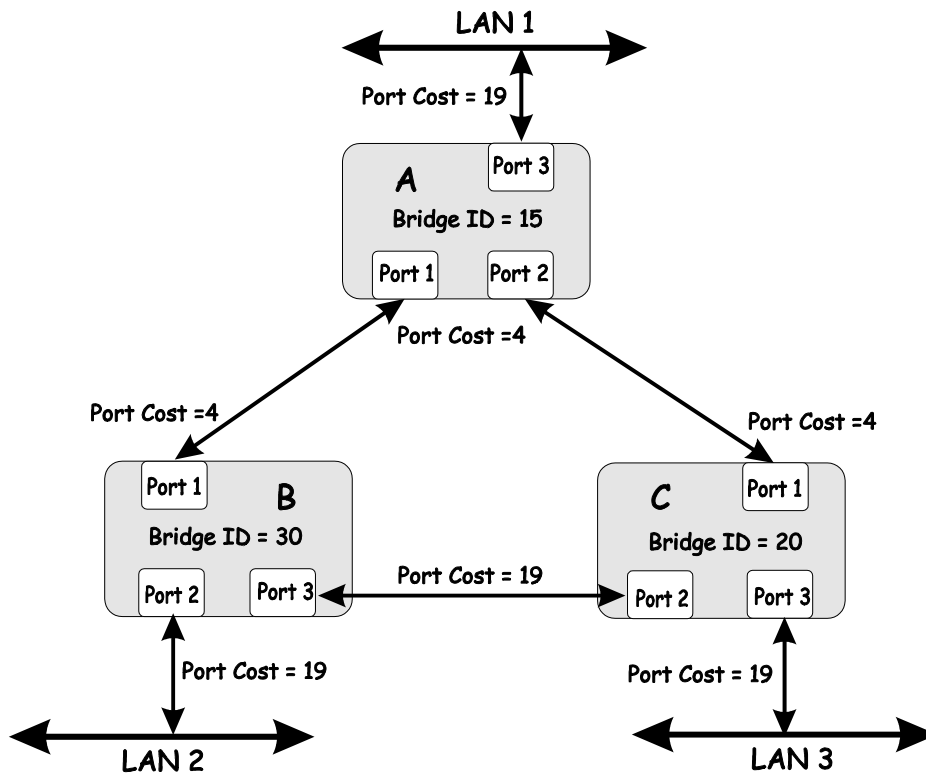


Figure 5-5. Before Applying the STA Rules

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

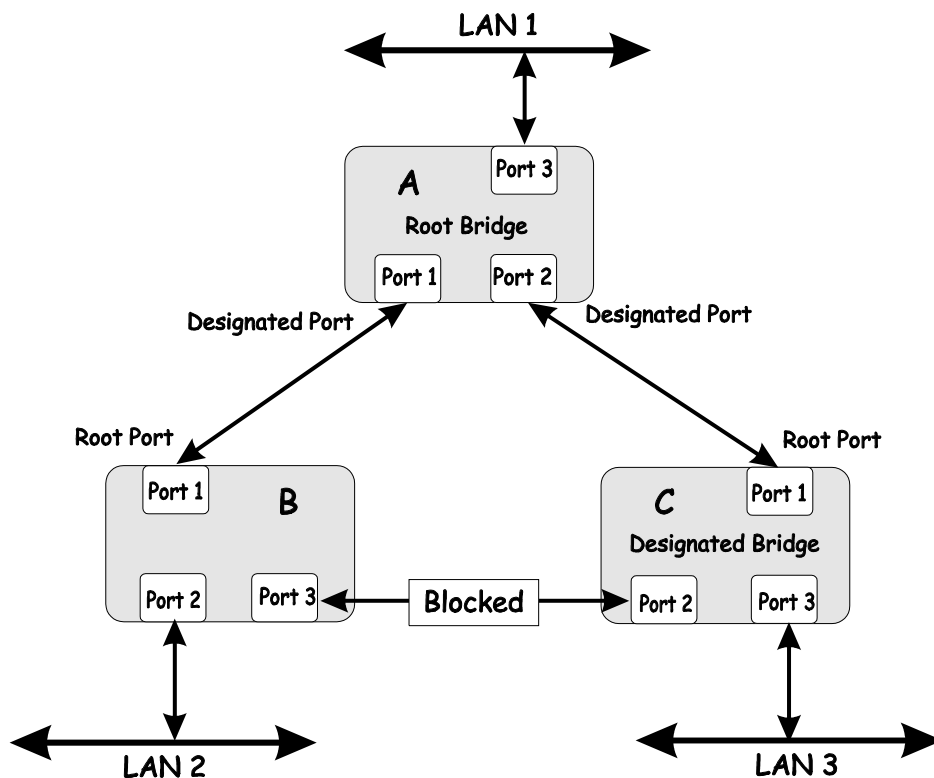


Figure 5-6. After Applying the STA Rules

### Sample Network using STP

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 packets that are forwarded only between ports within the VLAN.

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.

**Note:** A time saving feature called Asymmetric VLANs can be used by managers that do not require a complicated or overlapping VLAN setup. See details at the end of this section.

Within the Layer 2 switching environment, all end nodes are identified on the network by their unique MAC address. 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.

For VDSL applications, VLANs can be used for a group of ports used by a single subscriber. For example, one client may have a company network of a size that requires more than one port on the Switch. In this case, the Switch can be used to create one VLAN for the group of port leased the single subscriber. The client can then administer VDSL access on the private network as desired. All the ports within the client's VLAN can freely exchange packets through the VDSL Switch. Once the VLAN has been created, there should not be any more configurations decisions for the VDSL Switch manager, as long as there are no additional ports required by the client. If the client prefers to lease additional bandwidth (i.e. more ports), these can be easily added to the client's VLAN if there are unused ports available on the Switch.

The Switch 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.

By default the Switch assigns all ports to a single 802.1Q VLAN named DEFAULT\_VLAN. The DEFAULT\_VLAN has a VID = 1.

## IEEE 802.1Q VLANs

To help you understand 802.1Q VLANs as implemented by the Switch, it is necessary to understand the following:

**Tagging** - The act of putting 802.1Q VLAN information (a tag) 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 Switch. 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 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 Packet Forwarding Decisions

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.

## Packet Forwarding in 802.1Q VLANs

The diagram below illustrates packet forwarding decisions with 802.1Q VLANs.

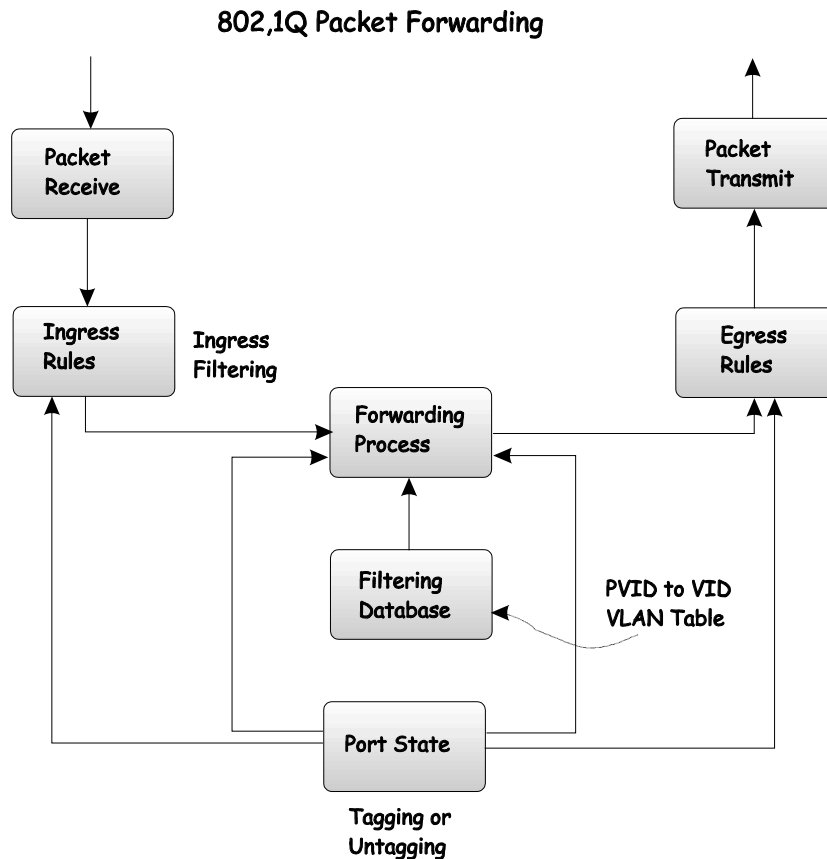


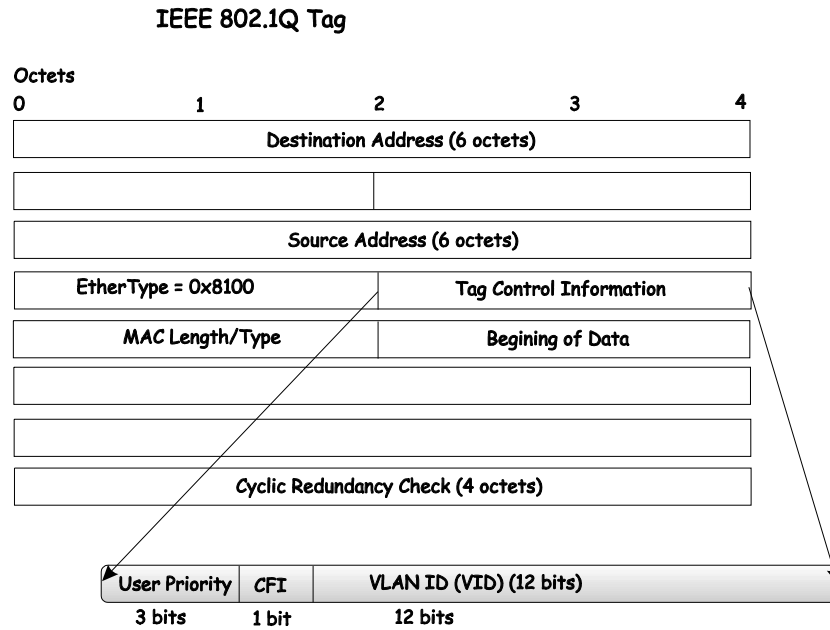
Figure 5-7. Packet Forwarding with VLANs

### 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.

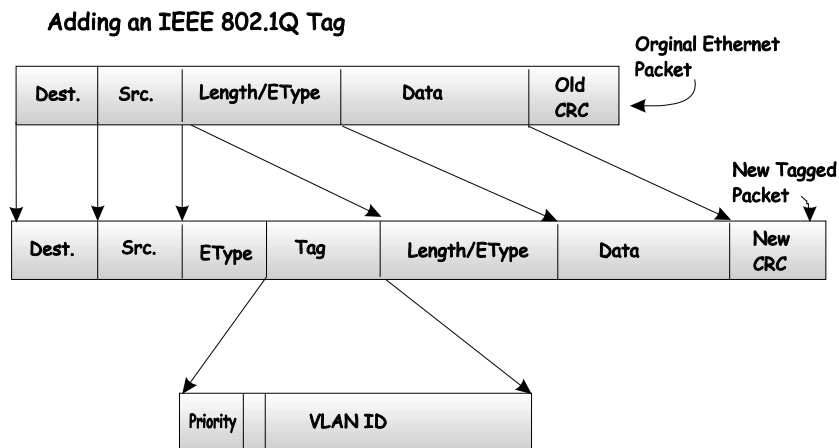
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information contained in the packet originally is retained.

The figure below illustrates the elements of the IEEE 802.1Q tag.



**Figure 5-8. 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 5-9. Adding 802.1Q Tag to a Packet Header**

### 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.

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 Packets***

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.

## **Configuring 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 be transmitted across VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

If no VLANs are configured on the switch 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.

## **Broadcast Storms**

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

Broadcast storms have long been a concern for network administrators with routers traditionally being used to prevent their occurrence, and if that failed, limit their scope. However, with the advent of VLANs, switches are now able to limit broadcast domains better and cheaper than routers. Also, many switches, including the DHS-3224V, have broadcast sensors and filters built into each port to further control broadcast storms.

## **Segmenting Broadcast Domains**

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

## **Eliminating Broadcast Storms**

SNMP agents can be programmed to monitor the number of broadcast packets on switch ports and act on the data. When the number of broadcast packets on a given port rise past an assigned threshold, an action can be triggered. When enabled, the rate of broadcast packets coming in through the affected port will be limited. Any traffic above the threshold limit will be discarded. The Switch also supports multicast storm control.

In the Switch, the default trigger threshold is set to 128,000 broadcast packets per second (128 Kbps) for both 100 Mbps Fast Ethernet ports and the optional 1000 Mbps Gigabit Ethernet ports. The thresholds can be set separately for the two types of ports and can easily be modified by using a normal SNMP management program or through the console interface.

## **Multicasting**

Multicasting enables a single network source to send packets to multiple destinations with persistent connections. The main advantage to multicasting is to decrease network load for communications that would otherwise use broadcasting.

## **Multicast Groups**

There are three types of IP v4 addresses: unicast, broadcast, and multicast. Unicast addresses are used to transmit messages from a single network device to another, single network device. Broadcast packets are sent to all devices on the subnetwork. Multicast defines a group of network devices or computers that will receive the multicast packets. The members of this group are not necessarily on the same subnetwork. Specially designated multicast addresses are used to send multicast packets to the group members.

## **Multicast Addressing**

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

## **Asymmetric VLANs**

Many network managers may not need an elaborate VLAN setup but still want to provide the added security of VLANs to the network. Asymmetric VLANs allow a manager to quickly and automatically set up a VLANs for single Switch or multiple Switch installations. The feature is enabled Switch wide and creates a unique VLAN for every client port. For cascaded Switch groups, a unique VLAN is created for each client port in the cascaded group. The VLANs created for the client ports each contain the client port, plus the uplink port as members. This creates a VLAN environment where each client port can freely link to the uplink port, but can not link to any other client port on the Switch or in the cascade group. See the section on configuring Asymmetric VLANs in Chapter 6 for an illustration of VLAN assignment using this feature.

## Configuring the Switch

The DHS-3224V Switch is configured using a console management interface. Any PC with a terminal emulator program can be used to manage the Switch out-of-band via the RS-232 console port. You can use this facility to perform many basic network management functions. In addition, the console program will allow you to set up the Switch for management in-band on a TCP/IP network using an SNMP-based network management system or Telnet. This chapter describes how to use the console interface to access the Switch, change its settings, and monitor its operation. Included in this chapter are the following:

- **Connecting to the Switch**
- **User Accounts Management**
- **Saving Changes**
- **Configuring the Switch**
- **Switch Utilities**
- Network Monitoring

### Connecting to the Switch

You can use the console interface by connecting to the Master Switch with a computer running an ordinary terminal emulator program (or VT100-compatible terminal). The console interface is an RS-232 serial port located on the front of the (Master) Switch. 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

**Note:** It may be convenient to configure the serial port settings as soon as you log in so the session does not log out during initial setup. To change the log out setting of the serial port, see the section **Serial Port Settings** in this chapter.

### Console Usage Conventions

The console interface makes use of the following conventions:

1. Items in *<angle brackets>* can be toggled between several choices using the space bar.
2. Items in *[square brackets]* can be changed by typing in a new value. You can use the backspace and delete keys to erase characters behind and in front of the cursor.
3. The up and down arrow keys, the left and right arrow keys, the tab key and the backspace key, can be used to move between selected items.
4. 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. The **Save Changes** function enters the current switch configuration into non-volatile RAM, and then reboots the Switch.

## Connecting to the Switch Using Telnet

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

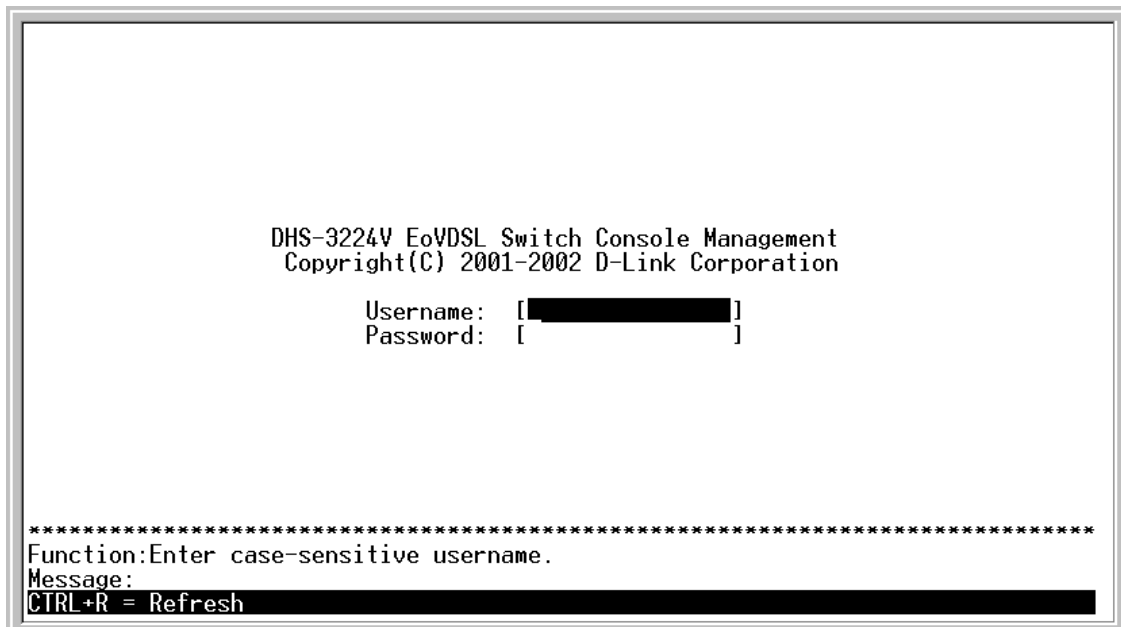
### First Time Connecting to the Switch

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 for first time log in.

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

```

DHS-3224V Local Management
-----
Main Menu

Basic Setup:                               Advanced Setup:

System Information                          Spanning Tree
Switch Information                         Unicast MAC Forwarding
Remote Management Setup                    Filtering
Switch Settings                           Priority
Configure Ports                           Multicasting
Setup User Accounts                        VLANs
Serial Port Settings                      VDSL Settings
Utilities                                  Port Trunking
Network Monitoring                         Port Mirroring
Save Changes
Reboot
Logout

*****
Function:Setup and browse switch information.
Message:
For Help, press F1
    
```

Figure 6- 2. Main menu (Access System Information Screen)

**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 **Setup User Accounts** from the main menu and press **Enter**:

```

DHS-3224V Local Management
-----
Main Menu

Basic Setup:                               Advanced Setup:

System Information                         Spanning Tree
Switch Information                        Unicast MAC Forwarding
Remote Management Setup                   Filtering
Switch Settings                          Priority
Configure Ports                          Multicasting
Setup User Accounts                       VLANs
Serial Port Settings                     VDSL Settings
Utilities                                 Port Trunking
Network Monitoring                        Port Mirroring
Save Changes
Reboot
Logout

*****
Function:Setup user account and password.
Message:
For Help, press F1
    
```

Figure 6- 3. Main Menu (Access User Accounts Menu)

The **Setup User Accounts** screen appears:

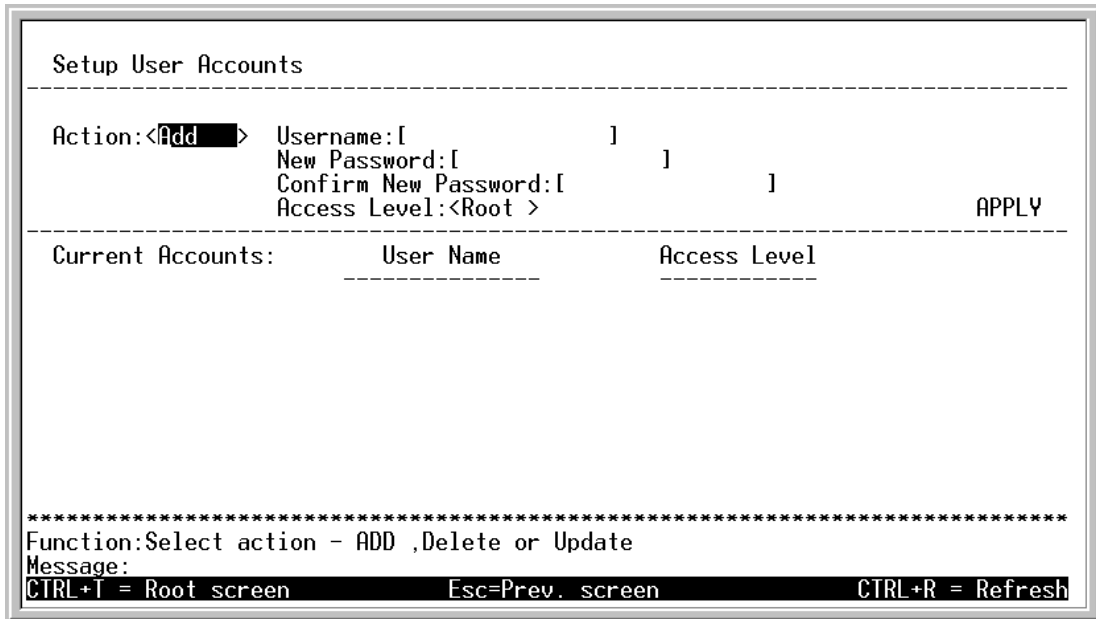


Figure 6- 4. Setup User Accounts Screen

To create user accounts:

1. 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 changes to be made to an existing user entry.
2. **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.
3. Highlight APPLY and press **Enter** to make the user addition effective.
4. Press **Esc.** to return to the previous screen or Ctrl+T to go to the root screen.
5. A listing of all user accounts and access levels is shown below the user setup menu. This list is updated when APPLY is executed.
6. 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:

<b>Switch Configuration</b>	<b>Privilege</b>		
<b>Management</b>	<b>Root</b>	<b>User+</b>	<b>User</b>
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
<b>User Accounts Management</b>			
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 DHS-3224V 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.

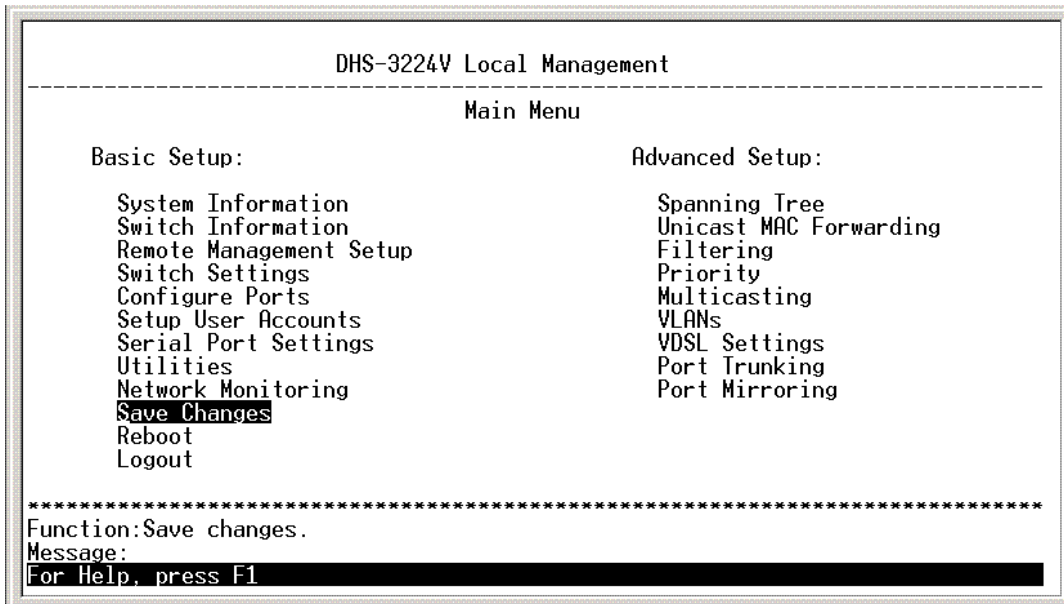


Figure 6- 5. Main menu

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

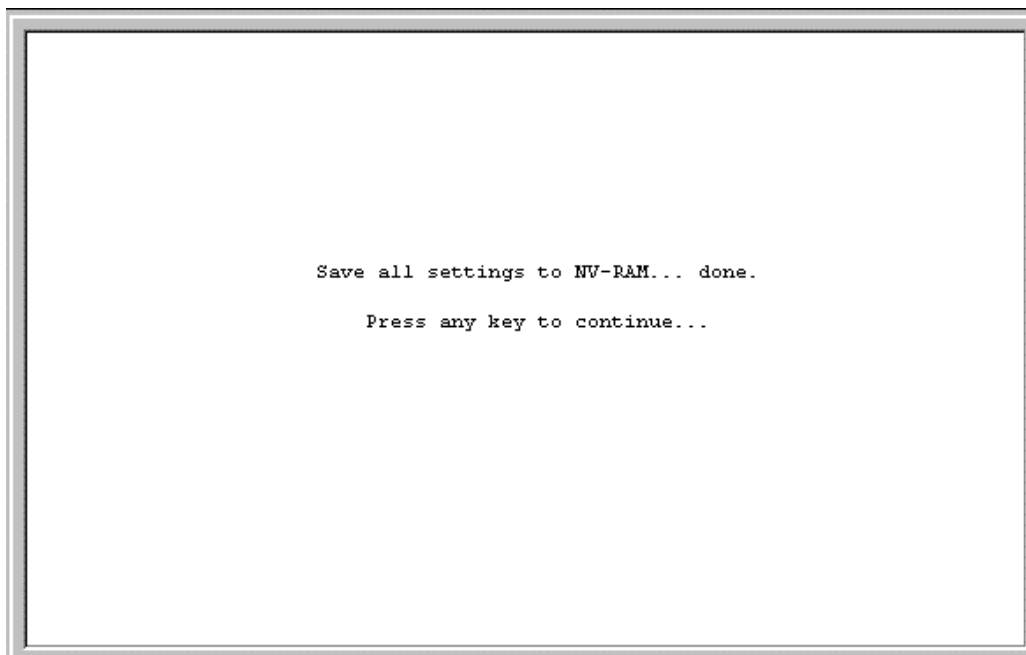


Figure 6- 6. Save changes Screen

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 B. These are the configuration settings entered at the factory and are the same settings present when the Switch was purchased.

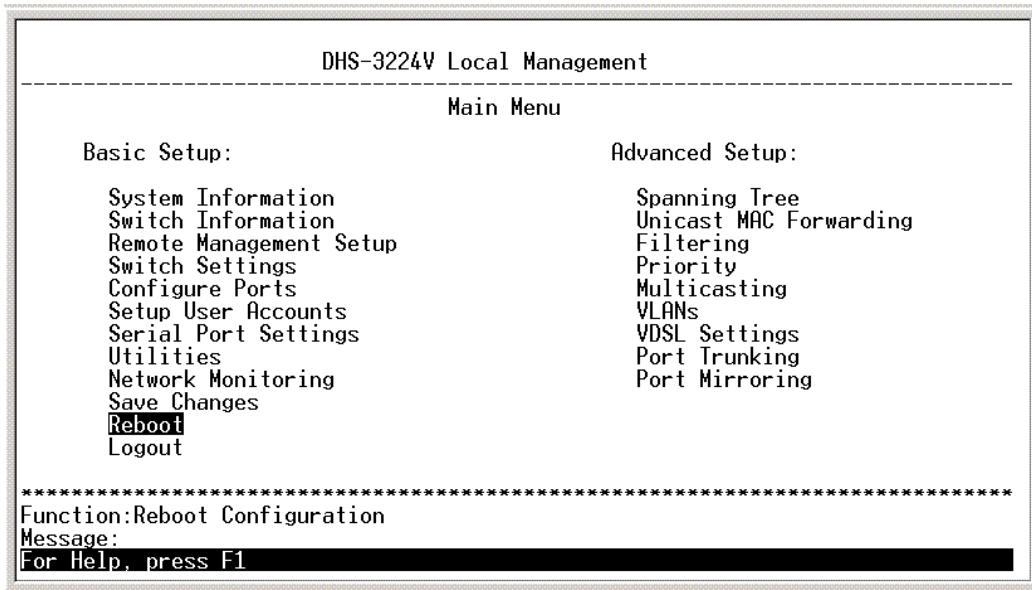


Figure 6- 7. Main Menu - Reboot

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

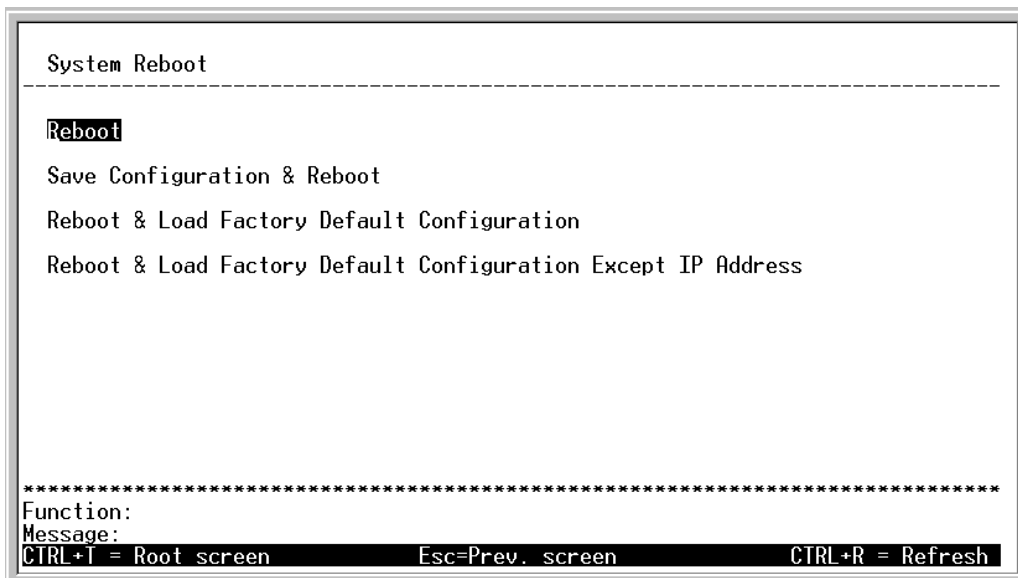


Figure 6- 8. System Reboot Menu

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 On to The Switch Console

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

1. Type in your **Username** and press **Enter**.
2. Type in your **Password** and press **Enter**.
3. The main menu screen will be displayed based on your 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 Accounts
-----
Action: <Add >  Username: [          ]
                New Password: [          ]
                Confirm New Password: [          ]
                Access Level: <Root >                                APPLY
-----
Current Accounts:      User Name      Access Level
                     -----
*****
Function: Select action - ADD ,Delete or Update
Message:
CTRL+T = Root screen      Esc=Prev. screen      CTRL+R = Refresh

```

**Figure 6- 9. Setup User Accounts Screen**

1. Toggle the **Action:<Add>** field using the space bar to choose **Add**, **Update**, or **Delete**.
2. Type in the **Username** for the user account you wish to change and enter the **Old Password** for that user account.
3. You can now modify the password or the privilege level for this user account.
4. 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.
5. If the privilege level is to be changed, toggle the **Access Level:<Root>** field until the appropriate level is displayed – **Root**, **User+** or **User**.
6. Highlight **APPLY** and press **Enter** to make the change effective.
7. 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

1. Toggle the **Action:<Add>** field to **Delete**.
2. **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.
3. Highlight **APPLY** and press **Enter** to make the deletion of the selected user take effect.
4. 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.

---

## Configuring the Switch

---

Switch management functions are grouped into two major groups in the console, Basic Setup and Advanced Setup functions. The remaining sections of this chapter deal with how you can use the console to setup these functions to implement an efficient network management strategy.

### Basic Setup

The Basic Setup features include:

#### System Information

*Stacking Configuration*

#### Switch Information

#### Remote Management Setup

*Setup Trap Recipients*

#### Switch Settings

#### Configure Ports

*Configure Port Settings*

*Configure Port Security*

*Configure Port Access Entity*

#### Setup User Accounts

#### Serial Port Settings

#### Utilities

*Upgrade Firmware*

*Use Configuration File on TFTP Server*

*Save Settings to TFTP Server*

*Save Log to TFTP Server*

*Ping*

*Local Loopback*

*Line Loopback*

#### Network Monitoring

*Port Utilization*

*Packet Error Statistic*

*Packet Analysis*

*Browse Address Table*

*IGMP Snooping Status*

*Switch History*

#### Save Changes

#### Reboot

#### Logout

### Advanced Setup

The Advanced Setup features include:

#### Spanning Tree

*Spanning Tree Settings*

*Port Spanning Tree Settings*

#### Unicast MAC Forwarding

#### Filtering

#### Priority

#### Multicasting

*Setup IEEE802.1q Multicast Forwarding*

*IGMP Snooping State*

#### VLANs

*Configure 802.1Q Port Settings*

*Edit 802.1Q VLANs*

*Configure Asymmetric VLAN*

#### VDSL Settings

#### Port Mirroring

## Serial Port and SLIP Settings

To change the serial port settings, highlight **Serial Port Settings** on the Main Menu and press **Enter** to see the following screen:

```

Serial Port and SLIP Settings
-----
Serial Port Setting:          SLIP Settings:
Baud Rate:<9600 >           Interface Name:
Data Bits:<8>                 Local IP Address:  0.0.0.0
Parity  :<None>              Remote IP Address: 0.0.0.0
Stop Bits:<1>                MTU: 1006
Auto-Logout:<Never >
Serial Port For:<Console>

APPLY

*****
Function:Select auto logout timer.
Message:
CTRL+T = Root screen      Esc=Prev. screen      CTRL+R = Refresh

```

**Figure 6- 10. Serial Port and SLIP Settings Screen**

Select either the **Serial Port Settings** or **SLIP Settings**.

The following Serial Port Settings fields can then be set:

- **Baud Rate** - Sets the serial bit rate that will be used to communicate the next time the Switch is restarted. Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are **2400, 9600, 19,200** and **38,400** bits per second. The default setting is **9600**.
- **Data Bits** – Toggle to select **7, 8**
- **Parity** – Toggle to select **None, Odd, Even**
- **Stop Bits** - Toggle to select **1, 2**
- **Auto-Logout** - This sets the time the interface can be idle before the switch automatically logs-out the user. The options are **2 mins, 5 mins, 10 mins, 15 mins**, or **Never**.

## Switch Information

Choose **Switch Information** to access the first item on the **Main Menu** and press **Enter**. The following menu appears:

```

Switch Information
-----
Unit : <1>
MAC Address           : 00-05-5D-ED-85-2F
Ext.Module Type       : 10/100 TX 1 Port Module
Ext.Module Version    : 2A1
VDSL Patch File Version : 0x0058
Fan Status            : Good

Stacking Configuration

*****
Function:Select the device.
Message:
CTRL+T = Root screen      Esc=Prev. screen      CTRL+R = Refresh
    
```

**Figure 6- 11. Switch Information Menu**

Use the Switch Information menu to view information about any unit in the stack. Toggle **Unit : < >** to select any Switch in the stack according to its number in the stack order (1 – 6), where unit number 1 is the master of the Switch stack.

The read-only information that can be viewed in the Stacking Information Window is as follows:

<b>MAC Address</b>	MAC address of the Switch
<b>Ext. Module Type</b>	Type of module (Extension Module) used for uplink to Ethernet backbone
<b>Ext. Module Version</b>	Version number of the Extension Module
<b>VDSL Patch File Version</b>	Version number of the VDSL Patch File
<b>Fan Status</b>	Current status of system fan, <i>Good</i> or <i>Fail</i>

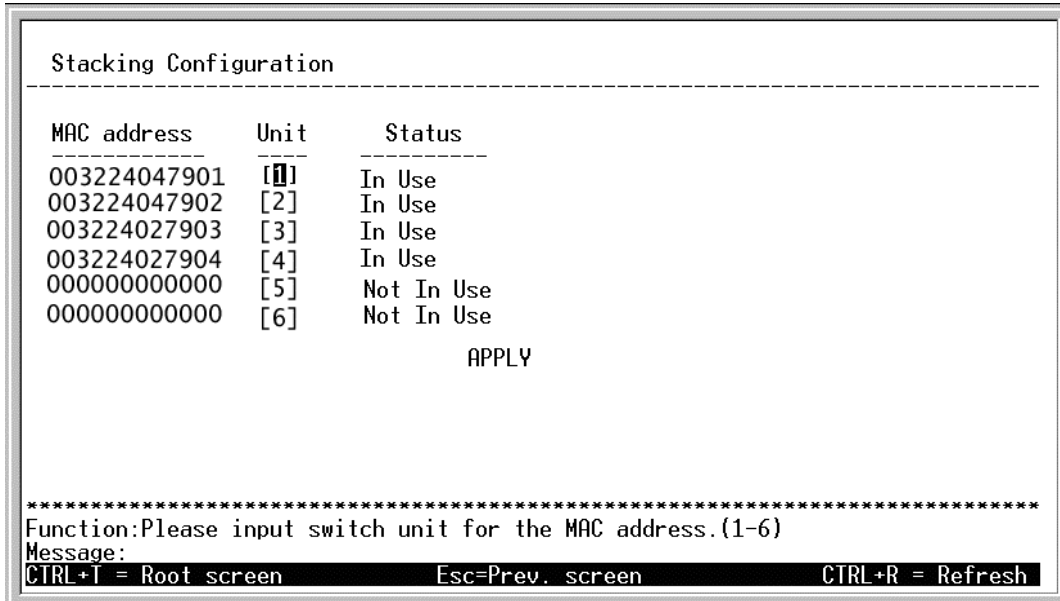
**Note:** If the Master Switch is changed, for any further configuration, it will be necessary to attach the serial cable to the new master after restarting the original master Switch. It is also recommended that you connect the Ethernet uplink to the new master.

This information is helpful to keep track of updates and to obtain the Switch's MAC address for entry into other network device's address table – if necessary.

To view or change the current configuration of the Switch stack hierarchy, select **Stacking Configuration** to view a new menu.

## Stacking Configuration

Access the Stacking Configuration menu Switch Information menu. The Stacking Configuration menu can be used to change the stack order. Choose **Stacking Configuration** and press **Enter**. The following menu appears:



**Figure 6- 12. Stacking Configuration Screen – (Auto-detect)**

The Stacking Configuration menu lists the following information regarding the Switch stack:

<b>MAC Address</b>	MAC address of Switch in stack
<b>Unit</b>	Stack order number of the Switch, this can be user defined.
<b>Status</b>	Switch can be either <i>In Use</i> or <i>Not in Use</i>

If you are using the auto-detect feature to determine stack order, the Switch stack will be listed from top to bottom in the hardware-determined order. The Master Switch (the lowest MAC address) is unit 1, the next highest MAC address is unit 2 and so on. If you have changed the stack order, the stack order appears in the order you have determined with the Master Switch (Unit 1) appearing at the top of the list.

To change the logical stack order of the Switch stack, highlight the unit you want to change and type in the new order number. Keep in mind that the Switch designated as Unit 1 will be the Master Switch. When the stack order number for each Master Switch is entered, highlight **APPLY** and press **Enter**. You must save the changes and restart the current Master Switch to achieve the new stack order. If you are changing the current Master Switch, you must reconnect the serial cable to the new Master Switch after saving the changes and rebooting. It is recommended that the Master Switch be used to uplink to the Ethernet backbone. Therefore, you should also change the uplink connection to the new Master Switch.

Each Switch in the stack must be restarted in order to implement the change to the stack order. Once you have saved the new stack order configuration and rebooted all the Switches in the stack, the new logical stack order will be displayed in the Stacking Configuration screen in the order.

**IMPORTANT:** All Switches in the stack must be restarted when the stack order is changed, even if the change is hardware-determined. For example, if the stack order is hardware-determined and Switches are added to or taken out of the stack, each Switch should be rebooted to implement the new stack order. Keep in mind that the Switch with the lowest value MAC address in the new stack arrangement will be the Master Switch after rebooting.



## System Information

Choose **System Information** to access the first item on the **Main Menu** and press **Enter**. The following menu appears:

```

System Information
-----
Device Type       : D-Link DHS-3224V Ethernet over VDSL Switch
Boot PROM Version : 1.00-B02
Firmware Version  : 1.01-B27
Hardware Version  : 3A1

System Name       : [DHS-3224V VDSL Switch Master 1      ]
System Location   : [201 South Park                      ]
System Contact    : [Rock A. Billy BR5-49                ]

                                Setup System Time      APPLY

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

**Figure 6- 13. System Information Menu**

The **System Information** menu displays the switch type, which (if any) external modules are installed, and the Switch's **MAC Address** (assigned by the factory and unchangeable). In addition, the **Boot PROM**, **Firmware**, **Hardware**, **Extension Module**, and **VDSL Patch Version** numbers are shown. This information is helpful to keep track of updates and to obtain the Switch's MAC address for entry into other 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 be listed here. Highlight **APPLY** and press **Enter** to make the change effective.

Use **Setup System Time** to set the system clock. Highlight Setup System Time and press **Enter**.

```

Setup System Time
-----

Current System Time:

    Date: 2000/00/00

    Time: 00:00:00

New System Time:

    Date: 20[021]/[031]/[12]

    Time: [15]:[00]:[00]

                                APPLY

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

**Figure 6- 14. Setup System Time Menu**

Enter the date and time, Highlight **APPLY** and press **Enter** to enter the system time information.

## 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:

Some settings such as the Switch IP address and subnet mask must be entered to allow the switch to be managed from an SNMP-based Network Management System or to be able to access the Switch using the TELNET protocol or the WEB-based Manager. Please see the next chapter for Web-based network management information.

The Remote Management Setup menu lets you specify how the switch will be assigned an IP address to allow the switch to be identified on the network. In addition, you may specify a subnet mask and default gateway.

Highlight Remote Management Setup to access the first item on the Configuration menu. The following screen appears:

```

Remote Management Setup
-----
Current Switch IP Settings:           Management Station IP Settings:
Get IP From:      Manual              IP Address:[0.0.0.0   ]
IP Address:      10.90.90.90          IP Address:[0.0.0.0   ]
Subnet Mask:     255.0.0.0           IP Address:[0.0.0.0   ]
Default Gateway: 0.0.0.0
Management VID:  1

New Switch IP Settings:              SNMP Community Settings:
Get IP From:      <Manual>           Community String Rights Status
IP Address:      [10.90.90.90   ]   lpublic          l<Read> <Enabled >
Subnet Mask:     [255.0.0.0     ]   lprivate         l<R/W > <Enabled >
Default Gateway: [0.0.0.0       ]   [                l<Read> <Disabled>
Management VID:  [1             ]   [                l<Read> <Disabled>

                                SETUP TRAP RECEIVERS    APPLY

*****
Function:Get IP from Manual, BOOTP or DHCP.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh
    
```

Figure 6- 15. Remote Management Setup Screen

The fields listed under the New Switch Settings heading are those that are currently being used by the switch. Fields that can be set include:

- **Get IP Address From** Determines whether the Switch should get its IP Address settings from the user (Manual), a BOOTP server, or a DHCP server. If Manual is chosen, the Switch will use the IP Address, Subnet Mask and Default Gateway settings defined in this screen after saving the changes and rebooting. If BOOTP is chosen, 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 get its IP settings from the BOOTP server upon being rebooted. If DHCP is chosen, a Dynamic Host Configuration Protocol request will be sent when the Switch is rebooted.
- **IP Address** Determines the IP address used by the Switch for receiving SNMP and telnet communications. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. This address should be a unique address on a network assigned to you by the central Internet authorities. The same IP address is shared by both the SLIP and Ethernet network interfaces.
- **Subnet Mask** Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. If no subnetting is being done, the value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network.

- **Default Gateway** IP address that determines where frames with a destination outside the current IP 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 inter-network, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
- **Management VID** Allows a management VLAN ID (VID) number to be set to allow management from a host within that VLAN to use either TELNET or the Web-based network manager. The default VID is 1 which includes the entire network until VLANs are configured.

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

### Management Station IP Settings

The Switch allows you to select up to three management stations used to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management access through the web manager or Telnet session. To define a management station IP setting, type in the IP address in the area provided, highlight APPLY and press **Enter**.

### Setting Trap Receivers

The Setup Trap Receivers feature allows the switch to send traps (messages about errors, etc.) to management stations on the network. Highlight Setup Trap Receivers in the Remote Management Setup screen and press **Enter**. The trap recipients can be setup from the following screen:

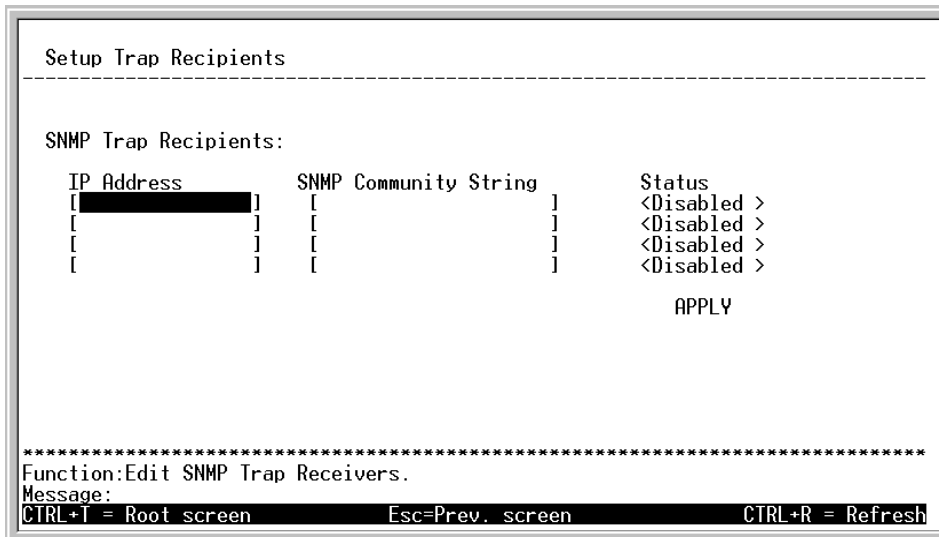


Figure 6- 16. Setup Trap Recipients Menu

Fields that can be set in the Setup Trap Recipients menu include:

- **IP Address** The IP address of a management station (usually a computer) that is configured to receive the SNMP traps from the switch.
- **SNMP Community String** Similar to a password in that stations that do not know the correct string cannot receive or request SNMP information from the switch.
- **Status** Toggle between <Enabled> and <Disabled> to enable or disable the receipt of SNMP traps by the listed management stations.

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

## Configure Switch Settings

Select **Switch Settings** menu and press **Enter** to access the following screen:

```

Switch Settings
-----
Switch Settings:
MAC Address Aging Time(sec):[300 ]
Switch 802.1x:<Disabled>
VDSL Rate Adaptive:<Enabled >

Broadcast/Multicast Storm Control:

Broadcast Storm Mode:<Disabled>
Multicast Storm Mode:<Disabled>

APPLY

*****
Function:Set the aging time(10-1000000) of MAC address entries.
Message:
CTRL+I = Root screen      Esc=Prev. screen      CTRL+R = Refresh

```

Figure 6- 17. Switch Settings Menu

## Switch Settings

The following fields can then be set:

- **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 to soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table.

- **Switch 802.1x:<Disabled >** Use this to enable or disable IEEE 802.1x Port Based Access Control for the Switch.
- **VDSL Rate Adaptive:<Enabled>** This must be enabled if you use the Rate Adaptive feature when you configure port settings.

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

## Broadcast/Multicast Storm Control

Use the entry fields described below for the parameters that control how the switch will react to broadcast and multicast storms.

- **Upper Threshold for Base Ports** This is the number of Broadcast/Multicast in Kbps received by the switch - on one of the base ports - that will trigger the switch's reaction to a Broadcast/Multicast storm.
- **Upper Threshold for Module Ports** This is the number of Broadcast/Multicast packets in Kbps received by the switch - on one of the module ports - that will trigger the switch's reaction to a Broadcast/Multicast storm.
- **Broadcast Storm Mode** Toggle to select Enabled or Disabled using the space bar to globally enable or disable the Switch's reaction to Broadcast storms, triggered at the threshold set above.
- **Multicast Storm Mode** This field can be toggled between Enabled and Disabled using the space bar. This enables or disables, globally, the switch's reaction to Multicast storms, triggered at the threshold set above for base and module ports.

## Configure Ports

Use the Configure Ports Screen to configure subscriber ports and port security.

To configure subscriber ports:

1. Highlight **Configure Ports** from the **Configuration** menu and press **Enter** to see the Configure Ports screen.
2. In the new window, highlight **Configure Port Settings**, **Configure Port Security** or **Configure Port Access Entity** to view those menus.

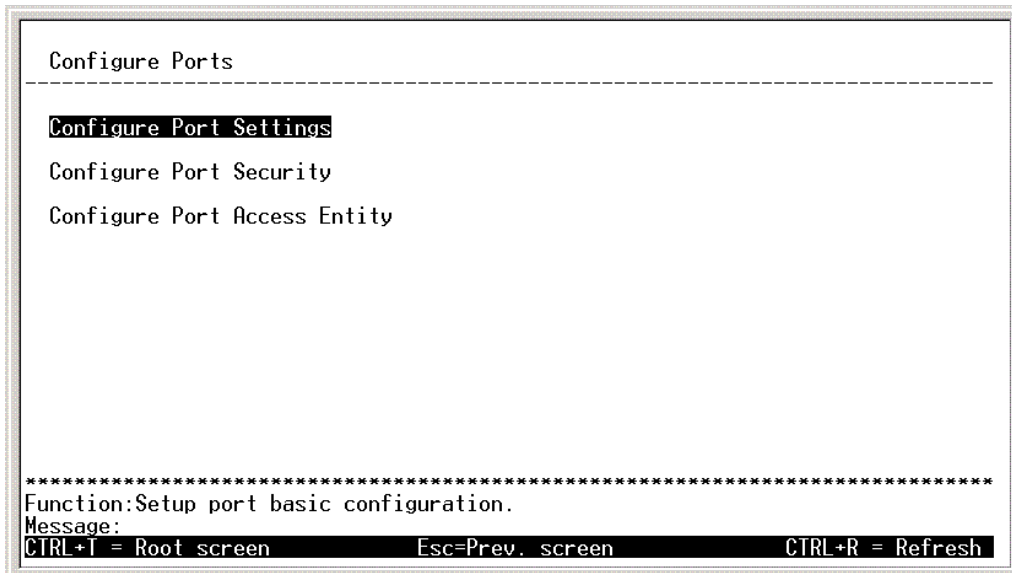


Figure 6- 18. Configure Ports

### Configure Port Settings

Use the Configure Port Settings Screen to enable subscriber ports and configure speed settings.

To configure subscriber ports:

1. Highlight **Configure Port Settings** from the **Configure Ports** menu and press **Enter** to see the Configure Ports screen.
2. The Configure Port Settings screen displays status information for each port.

Information for each subscriber port listed in the Configure Ports Screen includes:

<b>State</b>	Enabled or Disabled (Default = Enabled)
<b>DS/US Speed</b>	Download and Upload Speed can be customized for each port. Speeds for both (DS and US) can be set at 512 Kbps, 1Mbps – 15 Mbps in any symmetric or asymmetric combination. (Default = Mode 0, DS/US = 4Mbps/1Mbps).
<b>VDSL Connection</b>	The VDSL status information is presented as follows: Upstream Speed/ Downstream Speed/ Symmetry Condition.
<b>Ethernet Connection</b>	Ethernet connection status information applies to the Ethernet connection at the CPE and is displayed as follows: Connection Speed/Duplex Mode/Flow Control Method.
<b>Rate Adaptive</b>	The VDSL Rate Adaptive feature automatically senses line condition and adjusts DS/US speeds if a set rate cannot be maintained. The default setting will set speed to Mode 0 when a rate can no longer be supported. Optimum setting sets speed to Mode 0 but then tests raises the DS/US speed incrementally to achieve the best performance level.

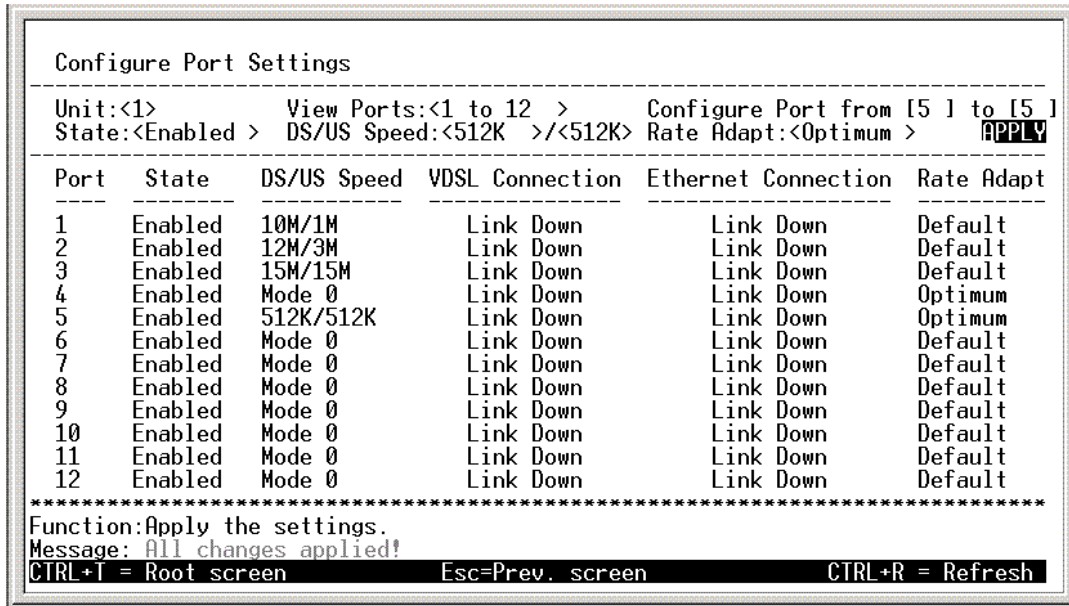


Figure 6- 19. Configure Port Settings Screen

For ports 1 – 24, configure the ports by selecting options described below:

Toggle the **Unit:<I >** to select the Switch and **View Ports:<I to I2 >**, using the space bar, to view the configuration of either ports 1 through 12, ports 13 through 24 or Slot-1. 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.

**DS/US Speed** can be toggled to select any available combination of download and upload speed. Default setting is *Mode 0*. Mode 0 has a DS/US Speed set to 4M/ 1M. If you press the space bar while the Speed is selected, the option changes to allow DS and US to be set separately. Speed for both DS and US may be changed to *512K, 1M, 2M, 3M,...* up to *15M*. Any changes to port speed must take into account the line distance to the CPE. VDSL Settings may also require adjustment (see 65 for VDSL Settings).

Toggle the space bar to set **Rate Adapt** to *Default, Optimum, and Disabled*.

To configure the uplink port, toggle to select **Toggle View Ports:** to select *<Slot-I>*. Toggle the **State: < >** field to either enable or disable the uplink. **Speed/Duplex** options for Slot-1 are *Auto, 100M/Full, 100M/Hal, 10M/Full* and *10M/Half*. **Flow Control** may be enabled or disabled in 10M/Full or 100M/Full.

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

## Configure Port Security

Port security can be configured for each subscriber port. Port security is used to limit the number of MAC addresses allowed on the port. Specify up to 16 MAC addresses allowed per port. This feature functions similar to a static forwarding table. For example, if you choose to allow 10 MAC addresses, the first 10 MAC addresses forwarded from that port are entered into a static table that never ages out. All packets originating from or destined for the port must contain one of the allowed MAC addresses (listed in the static table) in the header or it will be dropped.

To configure port security settings:

1. Highlight **Configure Port Security** from the **Configure Ports** menu and press **Enter** to see the Configure Port Security screen.
2. The Configure Port Security screen displays current security status of each port.

Information about each subscriber port listed in the Configure Port Security Screen includes:

<b>Port</b>	Subscriber port number
<b>Lock</b>	Enabled or Disabled (Default = Disabled)
<b>No. of MAC</b>	Number of MAC addresses allowed for the port

```

Configure Port Security
-----
Unit:<1>          View Ports:<1 to 12 >  Configure Port from [6 ] to [8 ]
                  Lock:<Enabled >      No. of MAC:[3 ]      APPLY
-----
Port      Lock      No. of MAC
-----
1         Enabled   9
2         Enabled   9
3         Enabled   6
4         Enabled   6
5         Enabled   6
6         Enabled   3
7         Enabled   3
8         Enabled   3
9         Disabled  -
10        Disabled  -
11        Disabled  -
12        Disabled  -
*****
Function:Apply the settings.
Message:
CTRL+F = Root screen      Esc=Prev. screen      CTRL+R = Refresh
    
```

**Figure 6- 20. Configure Port Security Screen**

Configure the ports by selecting options described below:

Toggle the **View Ports:<1 to 12 >** field, using the space bar, to view the configuration of either ports 1 through 12 or ports 13 through 24. To configure a specific port, toggle the **Configure Port from [ ] to [ ]** field until the appropriate port number or port range appears.

Toggle the **Lock: < >** field to enable or disable the port lock.

Type in the number of MAC addresses allowed in the **No. of MAC: [ ]** field. Up to 16 MAC addresses are allowed when the lock is enabled.

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



## Configure Port Access Entity

The DHS-3224V allows you to set the authentication status of individual ports on your Switch on the following menu.

Select **Configure Port Access Entity** on the **Configuration** menu and press **Enter**.

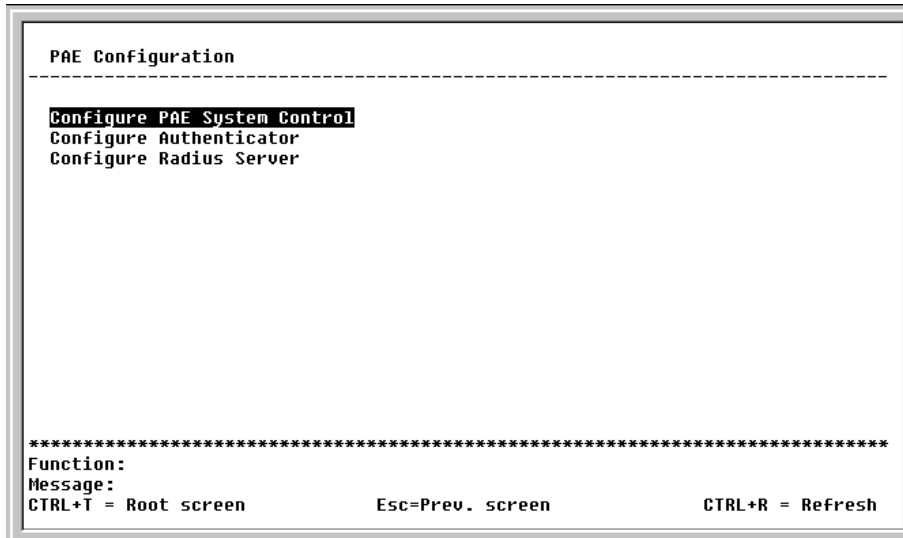


Figure 6- 21. PAE Configuration menu

## PAE System Configuration

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

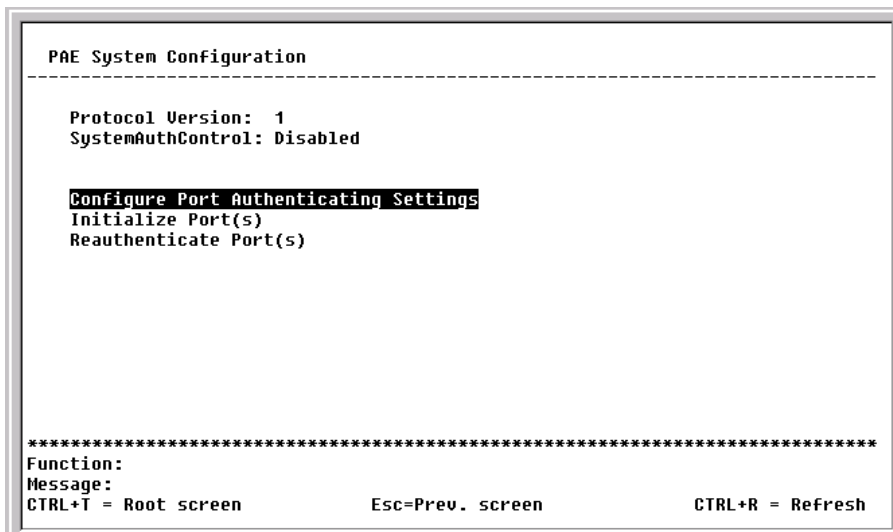


Figure 6- 22. PAE System Configuration menu

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.

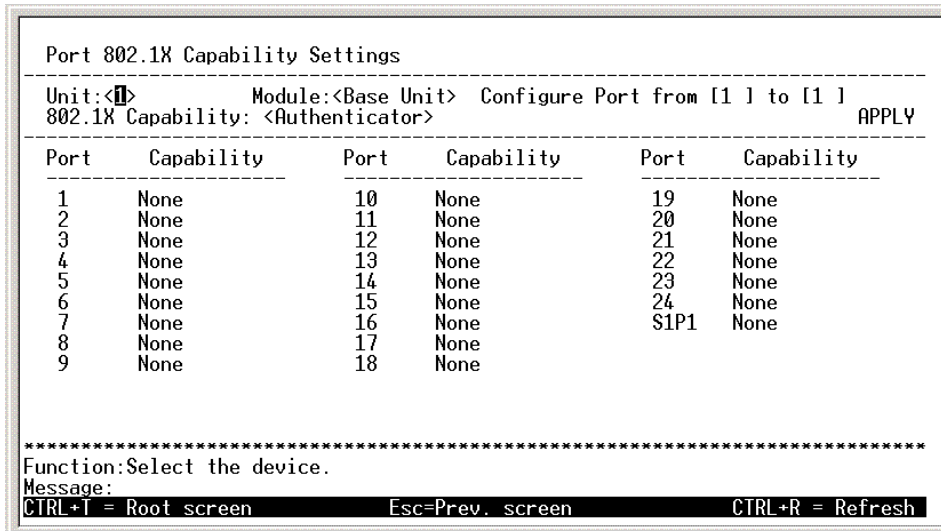


Figure 6- 23. Port 802.1X Capability Settings screen

To set up the Switch's 802.1X port-based authentication, toggle to select the **Module** :< > then 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.

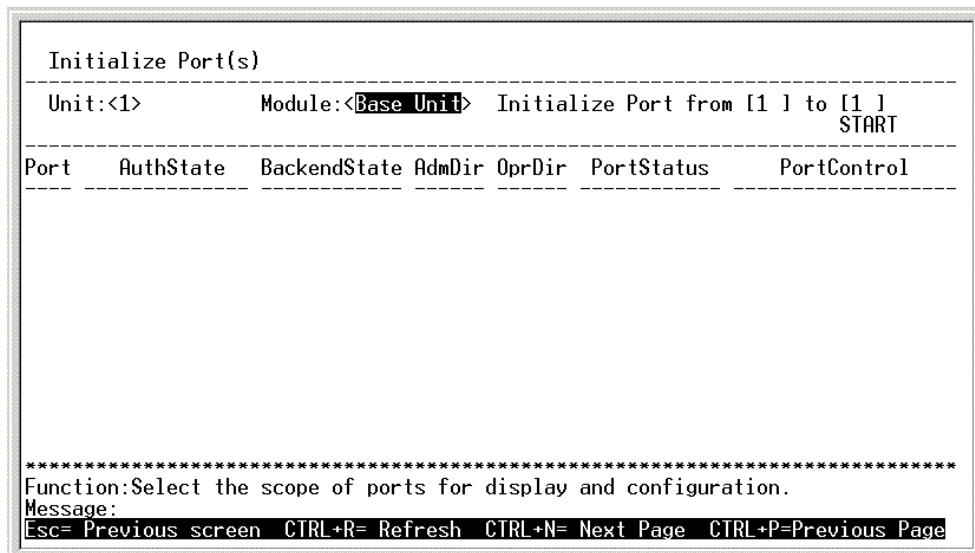


Figure 6- 24. Initialize Port(s) screen

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. To initialize ports, toggle to select the **Module** :< > then select which ports are to be initialized in the **Configure Port from [ ] to [ ]** field. Highlight START and press **Enter**.

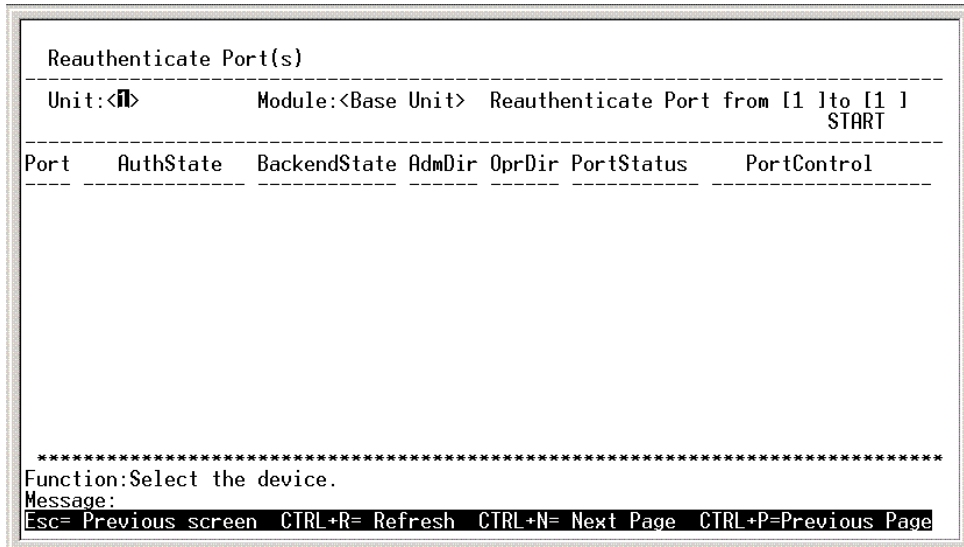


Figure 6- 25. Reauthenticate Ports(s) menu

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. To reauthenticate ports, toggle to select the **Module** :< > then select ports for reauthentication in the **Configure Port from [ ] to [ ]** field. Highlight START and press **Enter**.

### Configure 802.1X – Authenticator Configuration

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

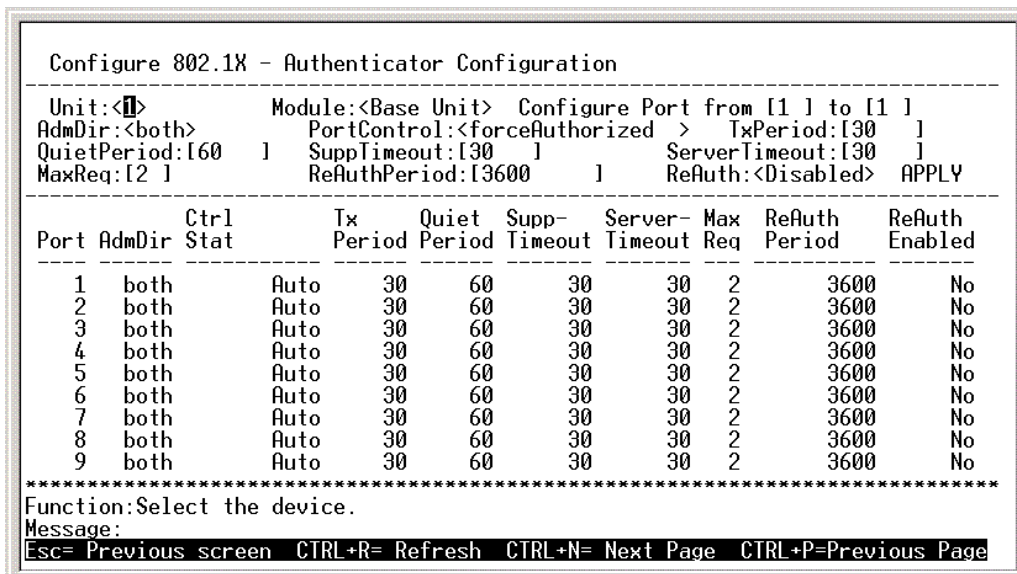


Figure 6- 26. Configure 802.1X – Authenticator Configuration screen

This screen allows you to set the following:

- **Unit:** < > - Toggle the unit in the stack order.
- **Module:** < > - Toggle to choose either the *Base Unit* for client ports or *Slot-1* for the uplink.
- **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. Each client attempting to access the network is identified (by the switch) according to the port through which the authentication message is relayed.
- **TxPeriod:**[30 ] – This sets the period of time for the authenticator PAE state machine.
- **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 sets the port's suppTimeout for the Backend Authentication state machine.
- **ServerTimeout:**[30 ] – This sets the port's serverTimeout for the Backend Authentication state machine.\*
- **MaxReq:**[2 ] – Set this for the Backend Authentication state machine.
- **ReAuthPeriod:**[3600 ] – Set this for the Reauthentication Timer state machine.
- **ReAuth:**<Disabled> – Toggle the port's re-authenticating control between *Enabled* and *Disabled*.

\* The *ServerTimeout* value must be set to a value that is less than the *Radius Timeout* and *Radius Maximum Retransmit* settings (see Configure General Radius Server Setting)

## Configure Radius Server

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

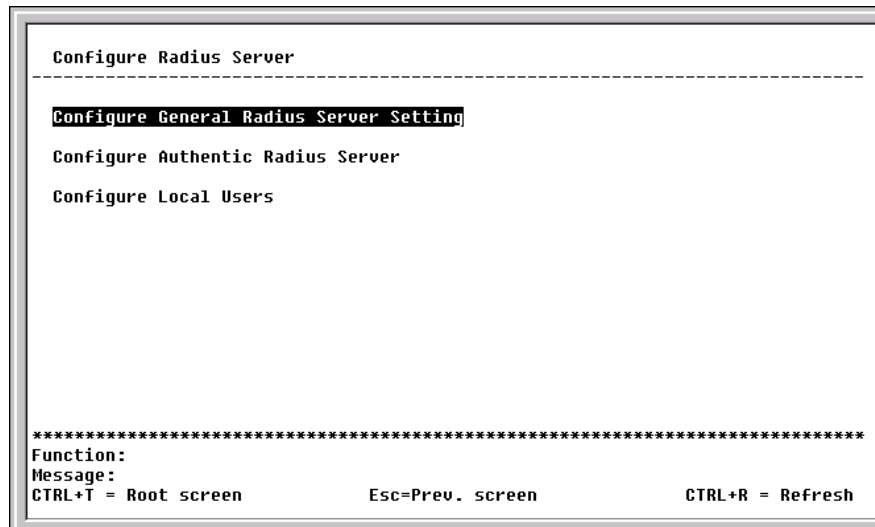


Figure 6- 27. Configure Radius Server menu

This menu offers three configuration choices for the radius server.

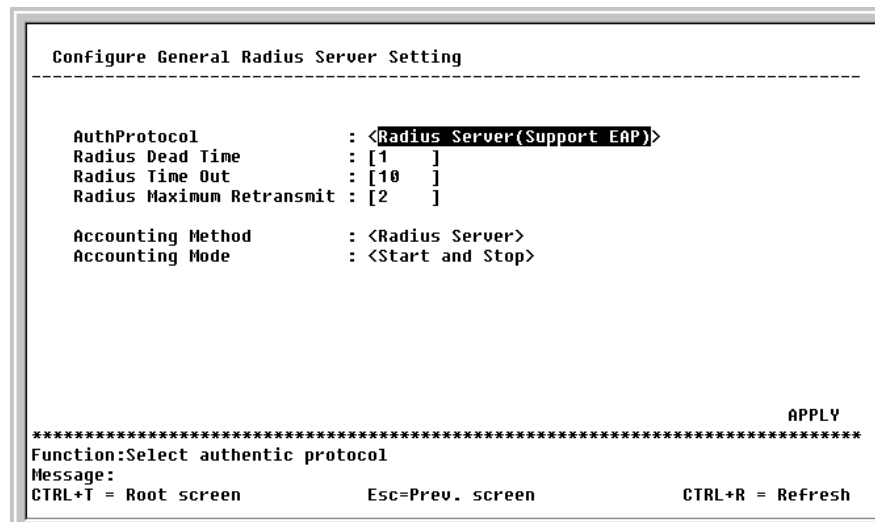


Figure 6- 28. Configure General Radius Server Setting screen

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*.
- **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*.
- \* The *ServerTimeout* value must be set to a value that is less than the *Radius Timeout* and *Radius Maximum Retransmit* settings (see Configure 802.1X – Authenticator Configuration)

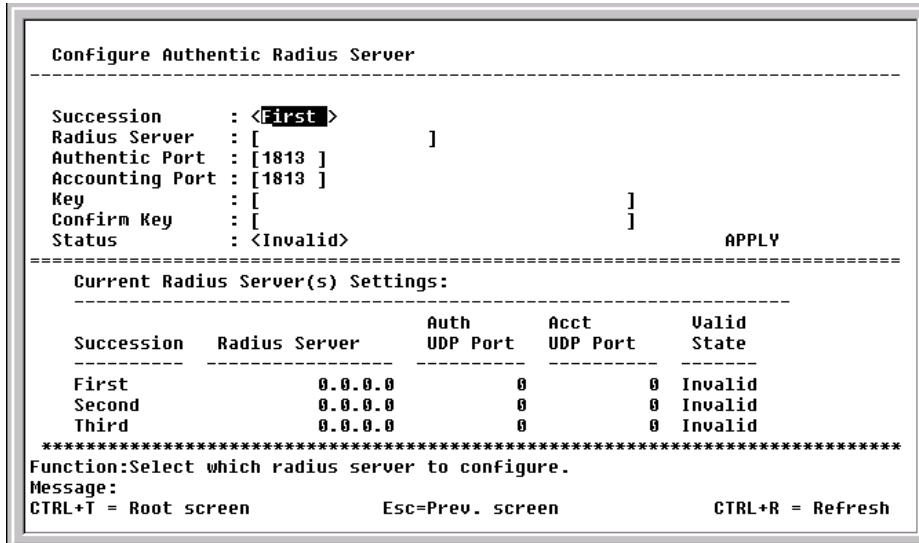


Figure 6- 29. Configure Authentic Radius Server screen

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:**[ *0* ] – Set the RADIUS account server(s) UDP port. The default is *1812*.
- **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.
- **Status:**<*Invalid*> –This allows you to set the RADIUS server as *Valid* or *Invalid*.

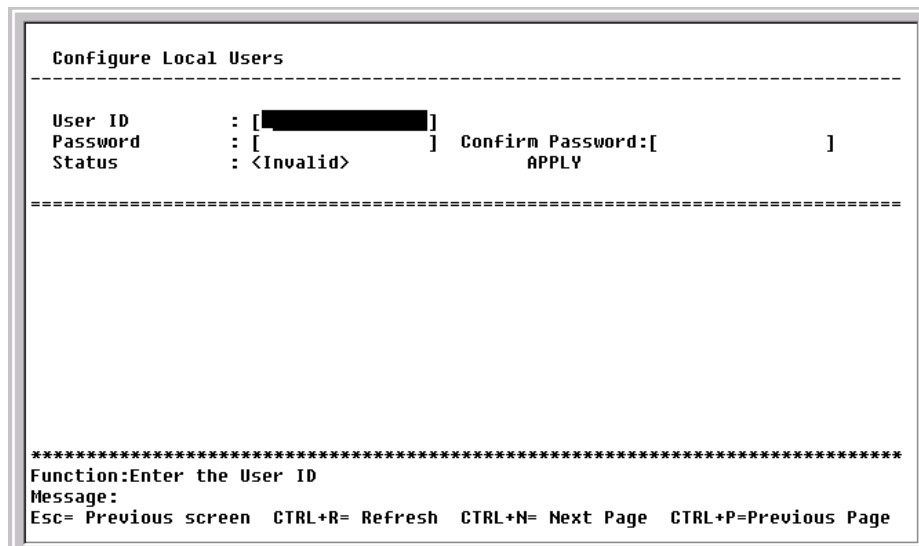


Figure 6- 30. Configure Local Users screen

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

## 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 **Port Mirroring** on the **Main Menu** to access the following screen:

```

Port Mirroring
-----
This feature allows you to mirror a port to another port for network
monitoring and troubleshooting purposes.

Source Port:Unit:<1>,Port:< 01 >
Source Direction:<Either >
Target Port:Unit:<1>,Port:< 09 >
Mirror Status:<Disabled>

      APPLY

*****
Function:Select the source device.
Message:
CTRL+I = Root screen      Esc=Prev. screen      CTRL+R = Refresh

```

**Figure 6- 31. Setup Port Mirroring screen**

To configure a mirror port:

1. Select the source port to mirror. Toggle to choose the **Source Port: Unit <>** and the **Port: <>**.
2. Choose the direction of the traffic to mirror from **Source Direction: <>**, toggle *Ingress*, *Egress* or *Either*.
3. Select the target port where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe. Toggle to choose the **Target Port: Unit <>** and the **Port: <>**.
4. Finally enable or disable port mirroring. Toggle **Mirror Status: <>** *Enabled* or *Disabled*.

**Note:** You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies.

## VDSL Settings

The VDSL Settings menu is used to change the Downstream Transmitting Power (DS Tx Power) for each port individually.

**IMPORTANT:** Before changing the default DS Tx Power setting, consider the following:

1. National or local telecommunications regulations may limit the range of settings that can be used.
2. Each Switch unit should use the same settings for all ports on the Switch.
3. Consider the effects of changing the DS Tx Power on upstream and downstream SNR.

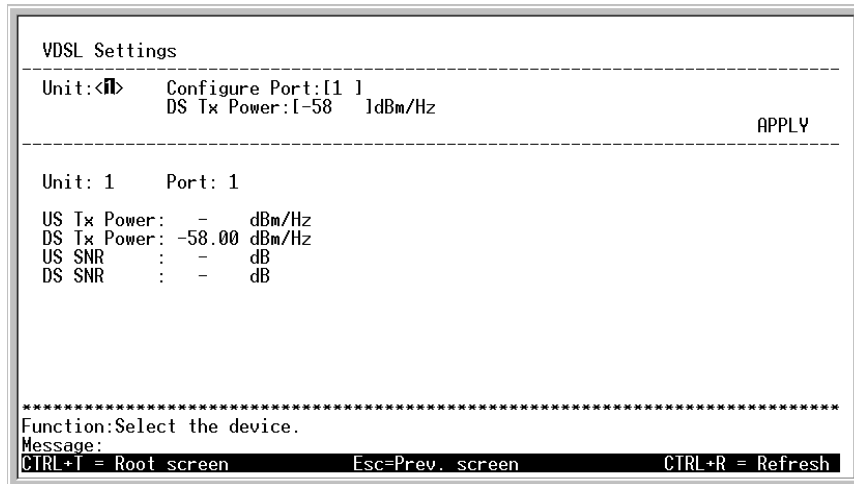


Figure 6- 32. VDSL Settings Menu

The default DS Tx Power value (-58 dBm/Hz) has been determined through testing to be the optimal value for maximum loop length. Increasing the DS Tx Power will increase the DS SNR but decrease the US SNR.

Enter the port number in the Configure **Port:**[ ] space. Enter a value (-90 dBm/Hz to -55 dBm/Hz) in the **DS Tx Power:**[ ] field. Highlight **APPLY** and press **Enter** to make the change effective.

### Configure Spanning Tree Protocol

The Spanning Tree Protocol is used to prevent loops in a network in which alternative connections exist between switches. The Protocol Parameters allow you to change the behind the scene parameters of the Spanning Tree Protocol at the bridge level.

### STP Parameter Settings

To globally configure the Protocol Parameters:

Choose Spanning Tree from the Main Menu appearing under Advanced Setup and press **Enter**. The following Spanning Tree menu will be displayed:

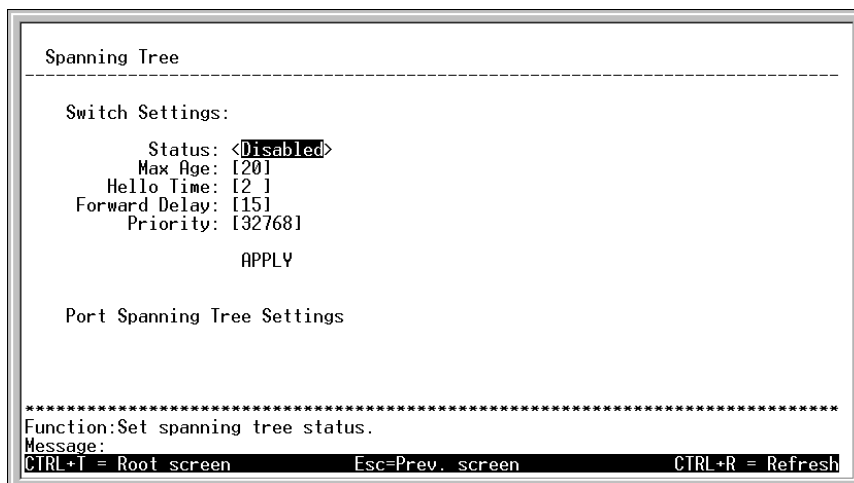


Figure 6- 33. Configure Spanning Tree Menu

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.

**Note:** Observe the following formulas when setting the above parameters:  
 Max. Age ≤ 2 x (Forward Delay - 1 second)  
 Max. Age ≥ 2 x (Hello Time + 1 second)

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

## Port Spanning Tree Settings

In addition to setting Spanning Tree parameters for use on the switch level, the DHS-3224V 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**.

The screenshot shows the 'Port Spanning Tree Settings' menu. At the top, it says 'View Ports: <1 to 12>' and 'Configure Port from [1] to [1]'. Below this is a table with columns: Port, Connection, Cost, Priority, and Status. The table lists ports 1 through 12, all with a cost of 19 and priority of 128, and all in a 'Forwarding' status. At the bottom of the screen, there are control instructions: 'Function: Select the scope of ports for display and configuration.', 'Message:', and 'CTRL+I = Root screen', 'Esc=Prev. screen', and 'CTRL+R = Refresh'. The word 'APPLY' is visible in the top right corner of the screen.

Port	Connection	Cost	Priority	Status
1	100M/Full/802.3x	19	128	Forwarding
2	-	19	128	Forwarding
3	-	19	128	Forwarding
4	-	19	128	Forwarding
5	-	19	128	Forwarding
6	-	19	128	Forwarding
7	-	19	128	Forwarding
8	-	19	128	Forwarding
9	-	19	128	Forwarding
10	-	19	128	Forwarding
11	-	19	128	Forwarding
12	-	19	128	Forwarding

**Figure 6- 34. Port Spanning Tree Settings Screen**

Toggle the **View Ports:**< > field to the range of ports to be configured. The ports are displayed for configuration in groups of 12. **Enter** the port number or port range in the **Configure Port from [ ] to [ ]** field.

The Port Group STP parameters that can be configured are:

- **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.
- **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.

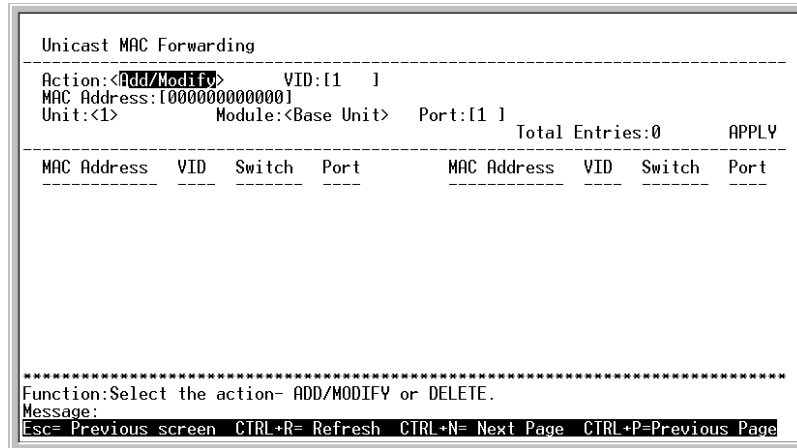
Highlight APPLY and press **Enter** to make the change effective.

## MAC Address Filtering and Forwarding

Use the Filtering and Forwarding menus to filter and forward unicast packets according to MAC address.

### Configure MAC Address Forwarding

To configure unicast MAC address forwarding, highlight Unicast MAC Forwarding in the Main Menu and press **Enter**:



**Figure 6- 35. Unicast MAC Forwarding Screen**

The **Action**:< > field can be toggled between **Add/Modify** and **Delete** using the space bar.

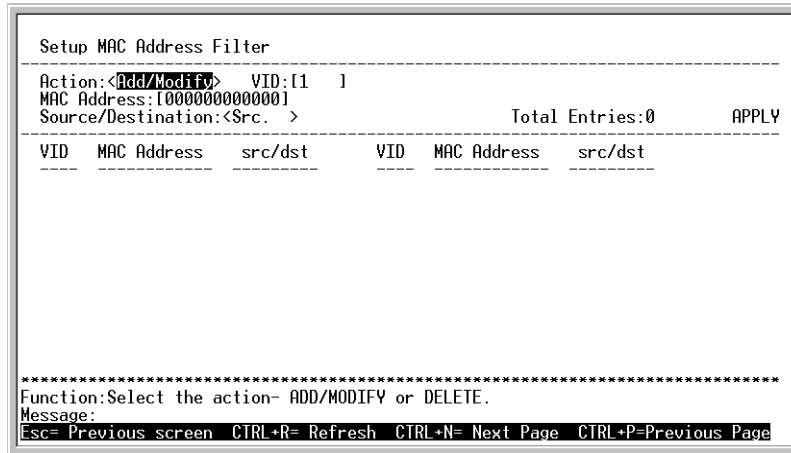
Enter the VLAN ID in the **VID**: [ ] field and the MAC address to be filtered in the **MAC Address**: [ ] field. This address must be a unicast MAC address.

The **Module**:< > field can be toggled between **Base Unit** (24 subscriber ports) and **Slot-1** (VDSL Uplink module). Enter the port number in the **Port**: [ ] field.

Highlight **APPLY** and press **Enter** to make the changes current. Use **Save Changes** from the **Main Menu** to save the changes to NV-RAM.

## Configure MAC Address Filtering

To configure unicast MAC address filtering, highlight Filtering in the Main Menu and press **Enter**:



**Figure 6- 36. MAC Address Filtering Screen**

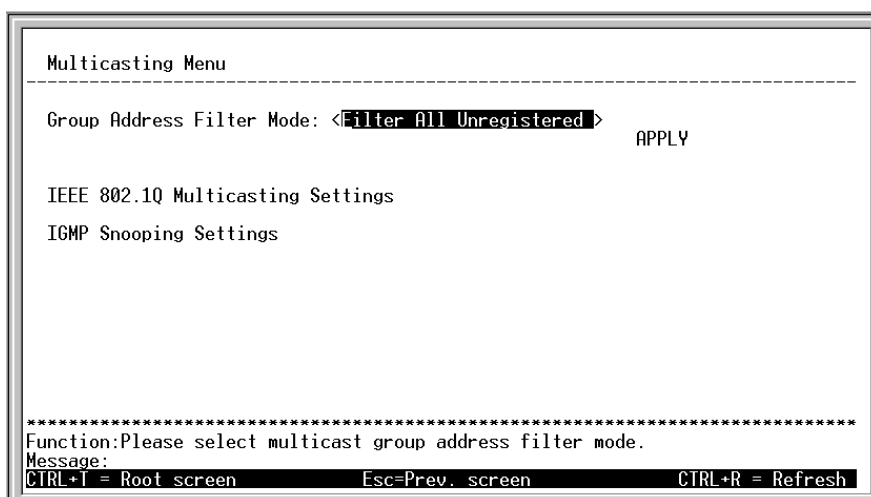
The **Action**:< > field can be toggled between **Add/Modify** and **Delete** using the space bar. Enter the VLAN ID in the **VID**:[ ] field and the MAC address to be filtered in the **MAC Address**:[ ] field.

The **Source/Destination**: < > field can be toggled between **Src.** (source), **Dst.** (destination), and **Either**. The MAC address entered into the filtering table can be filtered as a source (packets will not be received from the MAC address), as a destination (packets will not be transmitted to the MAC address), or as either a source or destination (packets will not be received from or transmitted to the MAC address).

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 Multicasting

To configure Multicasting on the Switch, Port Based or IEEE 802.1Q VLANs must already be defined on the Switch. The Multicasting Menu offers a configuration option for IEEE 802.1Q Multicasting and IGMP Snooping. This menu is also used to toggle group address filtering options. To access this menu highlight Multicasting on the Main Menu and press **Enter**:



**Figure 6- 37. Multicasting Menu Screen**

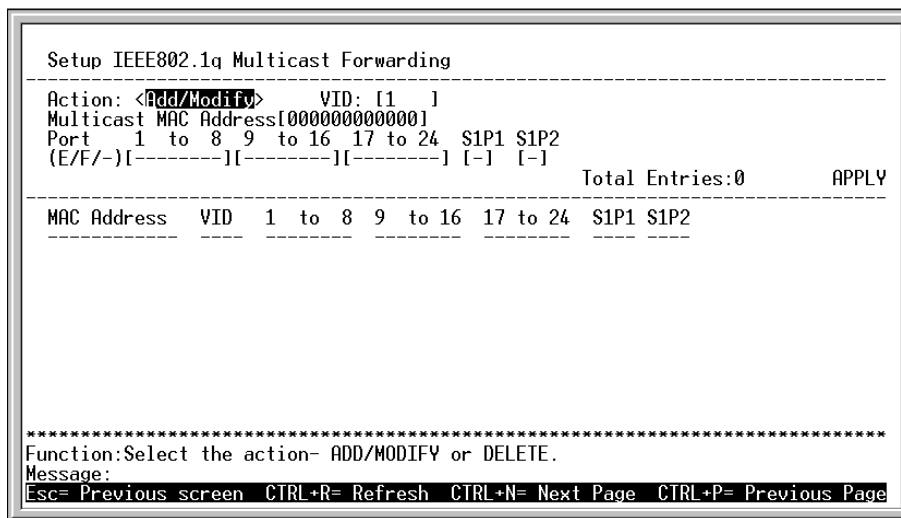
The Group Address Filter is used to customize filtering and forwarding of multicast packets for the entire Switch. A multicast packet is “registered” if its source address is listed in the multicast table. To change the Group Address Filter Mode, toggle the **Group Address Filter Mode:** < > to select:

- Filter All Unregistered**                      Filters all unregistered multicast packets.
- Forward All**                                      Forwards all multicast packets according to VLAN assignment.
- Forward All Unregistered**                  Forwards all unregistered multicast packets.

Select the filter mode option, highlight APPLY and press **Enter** to enable the option.

### Configure IEEE 802.1Q Multicast Forwarding

To edit the IEEE802.1 Multicast Forwarding settings highlight IEEE802.1Q Multicasting Settings from the Multicasting Menu and press **Enter**.



**Figure 6- 38. Multicast Forwarding Settings Screen**

Use the following fields to configure Multicast Forwarding settings:

- **Action** Toggle to select <Add/Modify> or <Delete> to add, change or delete an entry to the multicast forwarding table.
- **VID** For IEEE 802.1Q VLANs only. **Enter** the VID of the VLAN that will be receiving the multicast packets.
- **Multicast Address** **Enter** the multicast MAC address of the source, and then enter the member ports.

Each port can be an Egress, Forbidden, or a Non-member of the multicast group, on a per-VLAN basis.

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

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 between E, F, or - using the space bar. Use the following definitions to guide you:

- E** Egress membership 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.
- Non-member status 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 apply the Multicast Forwarding settings. Use the Save Changes menu to save the settings to NV-RAM.

## Configure IGMP Snooping

When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa.

IGMP Snooping is disabled by default. To enable IGMP Snooping and configure settings, highlight IGMP Snooping Settings in the Multicasting Menu and press **Enter**.

```

IGMP Snooping Settings
-----
IGMP Snooping State :<Enabled>
Querier State       :<Non-Querier>
Robustness Variable:[2 ]
Query Interval      :[125 ]
Max Response        :[10]
Age Out             :260
                    APPLY

Age Out = Robustness Variable * Query Interval + Max Response
*****
Function:Please select IGMP Snooping state.
Message:
CTRL+I = Root screen      Esc=Prev. screen      CTRL+R = Refresh

```

**Figure 6- 39. IGMP Snooping Menu**

The user-changeable parameters for IGMP Snooping are as follows:

- **IGMP Snooping State:**<Disabled> – Toggle to *Enabled* to implement IGMP Snooping.
- **Querier State:** <Non-Querier> - Choose V1 Querier for version 1 querier, V2 Querier for version 2 querier, or Non-Querier.
- **Robustness Variable:** [2] - The Robustness Variable field allows an entry of 2 to 255. Adjust this variable according to expected packet loss. In other words, if packet loss is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss.
- **Query Interval:** [125] - The Query field allows an entry between 1 and 9,999 seconds and defines the time between transmitting IGMP queries.
- **Max Response:** [10] - The Max-Response field allows an entry between 1 and 254 and defines the maximum time allowed before sending a response report to a query measured in units of 1/10 of a second. This is used to adjust the "leave latency", the time interval between the moment the last host leaves a group and when the routing protocol is notified there are no more members.
- **Age-out Timer** - Displays the time the Switch waits between IGMP queries.

Highlight APPLY and press Enter to apply the IGMP Snooping settings. Use the Save Changes menu to save the settings to NV-RAM.

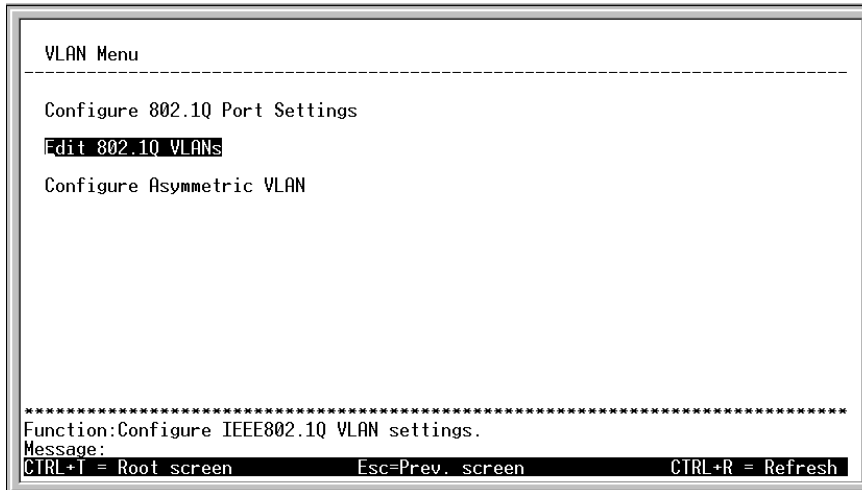
## Configure VLANs

If you wish to create an individual VLAN for each client port, read

**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.

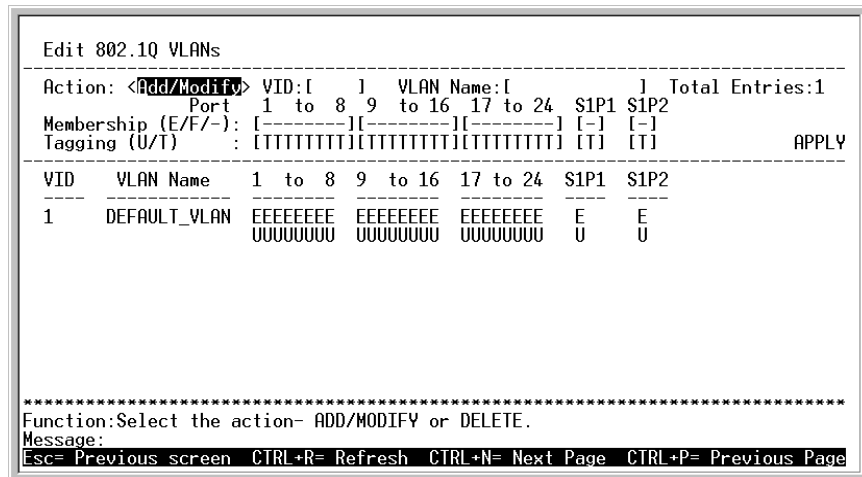
*To create a new 802.1Q VLAN:*

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



**Figure 6- 40. VLAN Menu**

To create an 802.1Q VLAN, highlight Edit 802.1Q VLANs and press **Enter**:



**Figure 6- 41. Edit 802.1Q VLANs Menu**

Create, change or delete an 802.1Q VLAN, using the following fields of the Edit VLANs Menu:

- **Action** Toggle to select <Add/Modify> or <Delete> to add, change or delete a VLAN.
- **VID** Assign a VLAN ID number for the VLAN group.
- **VLAN Name** Type in a name for the VLAN to be added, modified or deleted.

VLAN membership can be set individually for each port. At the same time, a port can be Tagged or Untagged.

*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 **Membership (E/F/ )**: [ || || ]. 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, F, or – 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.

**-** (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 **Tagging (U/T)**: [ || || ] 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.

Highlight **APPLY** and press **Enter** to make the change effective for the current session. To make enter the IP Interfaces into Non-volatile RAM, highlight **Save Changes** from the Main Menu and press enter.

**Example 802.1Q VLAN edit screen:**

```

Edit 802.1Q VLANs
-----
Action:<Add/Modify> VID:[2 ] VLAN Name:[Penthouse ] Total Entries:3
Unit:<1> Port 1 to 8 9 to 16 17 to 24 S1P1
Membership (E/-): [--EE----][-----][-----] [-]
Tagging (U/T) : [TTUUTTTT][TTTTTTTT][TTTTTTTT] [T] APPLY
-----
VID  VLAN Name  1 to 8  9 to 16  17 to 24  S1P1
-----
1    DEFAULT_VLAN  EEEEEEEE  EEEEE---  -----  -
      UUUUUUUU  UUUUUUTT  TTTTTTTT  T
2    Penthouse    --EE----  -----  -----  -
      TTUUTTTT  TTTTTTTT  TTTTTTTT  T
3    AAA Accounts  ---E---  --EEE---  -----  -
      TTTTUTTT  TTTTTTTT  TTTTTTTT  T
-----
*****
Function:Apply the settings.
Message: All changes applied!
Esc= Previous screen CTRL+R= Refresh CTRL+N= Next Page CTRL+P=Previous Page
    
```

**Figure 6- 42. Edit 802.1Q VLANs Menu**

**To configure the member ports of an 802.1Q VLAN:**

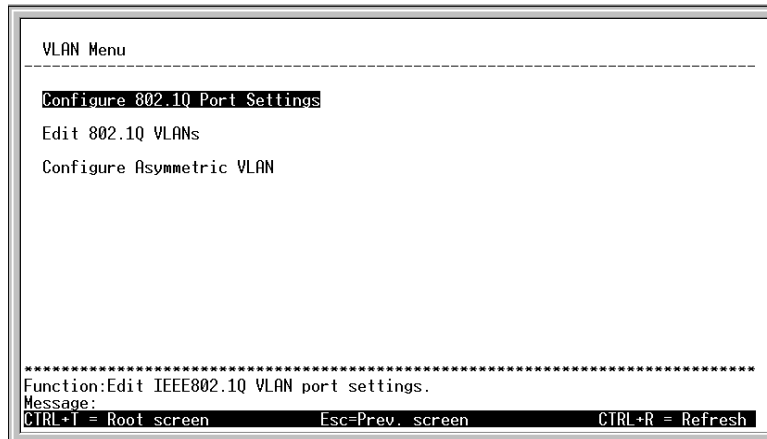


Figure 6- 43. VLAN Menu

Highlight Configure 802.1Q Port Settings and press **Enter**, the following screen will appear:

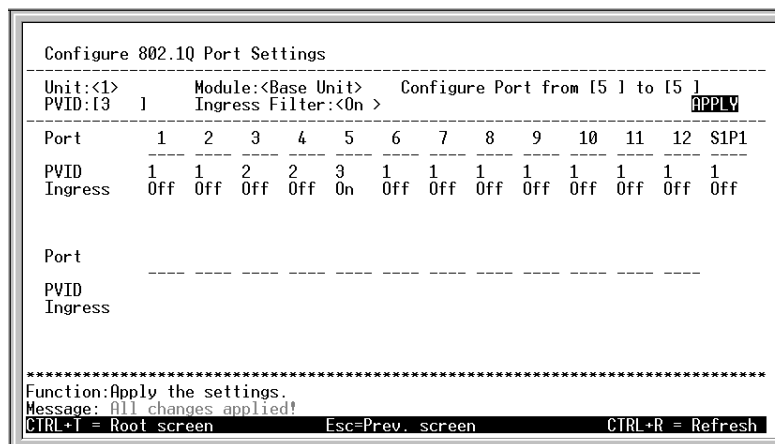


Figure 6- 44. Configure 802.1Q Port Settings Screen

Each port can be configured to use an Ingress Filter. The ports to be configured in a given session can be identified by either entering a range of port numbers or by entering the PVID#.

Ingress filtering is toggled between **On** and **Off** using the space bar.

**To configure a port's 802.1Q VLAN settings:**

Highlight the Configure Port from [ ] to [ ] field and enter the range of port numbers you want to configure. As an alternative you can use the arrow keys to highlight the PVID#[ ] field and enter the PVID for the VLAN's member ports you want to configure.

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

Use the arrow keys to highlight the remaining fields and the space bar to toggle between On and Off.

**Ingress Filter** – this 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.

**To edit an existing 802.1Q VLAN:**

1. Highlight VLANs on the main menu and press **Enter**.
2. Highlight Edit 802.1Q VLANs and press **Enter**.



3. Highlight the **Action:<Add/Modify>** field and toggle between **Add/Modify** and **Delete**. In the **Add/Modify** mode, both individual entries to a selected VLAN and entire VLANs can be added. In the **Delete** mode, entire VLANs can be deleted. VLANs to be edited can be selected by either the **VID#[ ]** field or the **VLAN Name:[ ]** fields. **Enter** either the VID or the VLAN Name for the 802.1Q VLAN you want to edit and press **Enter**.

**Note:** To delete an entire VLAN, toggle the **Action:<Add/Modify>** field to **Delete**, enter either the VID or the VLAN Name in the appropriate field and press **Enter**. Highlight **Apply** and press **Enter**. The selected VLAN will be deleted. To save the change into Non-volatile RAM, select **Save Changes** from the Main Menu.

The 802.1Q VLANs are edited by specifying which ports will be Egress Members, Forbidden non-members or non-members.

The ports are further set to be either a Tagged or an Untagged port.

**To edit the 802.1Q VLAN membership of a port:**

Highlight the first field of **Membership (E/F/-): [ ][ ][ ]**. 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, F, or – 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.

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

**To edit a port's Tagged or Untagged status:**

Highlight the first field of **Tagging (U/T):[ ][ ][ ]** 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.

Each port can be configured to have a PVID or to use an Ingress Filter.

**To configure a port's 802.1Q VLAN settings:**

Highlight the **Configure Port#[ ]** field and enter the port number of the port you want to configure. Use the arrow keys to highlight the **PVID#[ ]** field and enter the PVID for the port.

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

Use the arrow keys to highlight the remaining fields and the space bar to toggle between On and Off.

**Ingress Filter** – this 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.

## Asymmetric VLANs

Use Asymmetric VLANs to assign a unique PVID to each port on the Switch or stacked group. This may be a more convenient way to assign VLANs if you simply want to give each client port its own separate VLAN.

### To enable Asymmetric VLANs:

Highlight Configure Asymmetric VLANs and press **Enter**, the following screen will appear:

```

Configure Asymmetric VLAN
-----
Set the devices to VLAN configuration : <Auto>
                                     APPLY

Note: While the VLAN configuration is set, the following configuration
      would be changed.
      1. In 802.1Q VLANs, system will create VLAN for each VDSL port
         of 6 devices automatically.
      2. Uplink port's PVID will be assigned as 1 and the other VDSL
         ports will be assigned a unique PVID.

*****
Function:Auto/Clear asymmetric VLAN creation.
Message:
CTRL+I = Root screen      Esc=Prev. screen      CTRL+R = Refresh
    
```

Figure 6- 45. Configure Asymmetric VLANs Menu

To configure a Switch or stacked group for Asymmetric VLANs, toggle to select <Auto> from **Set the devices to VLAN configuration:<>**, highlight APPLY and press **Enter**.

When the changes are complete, you may view the new VLAN port assignments by pressing Esc to go back to the VLAN menu, and then highlight 802.1Q VLANs and press Enter.

```

Edit 802.1Q VLANs
-----
Action:<Add/Modify>  VID:[1 ]  VLAN Name:[DEFAULT_VLAN]  Total Entries:150
Unit:<1>             Port 1 to 8  9 to 16  17 to 24  $1P1
Membership (E/-):[EEEEEEEE][EEEEEEEE][EEEEEEEE] [E]
Tagging (U/T)   :[UUUUUUUU][UUUUUUUU][UUUUUUUU] [U]  APPLY
-----
VID  VLAN Name  1 to 8  9 to 16  17 to 24  $1P1
-----
1    DEFAULT_VLAN  EEEEEEEE EEEEEEEE EEEEEEEE  E
      UUUUUUUU  UUUUUUUU  UUUUUUUU  U
101  E-----  -----  -----  E
      UTTTTTTT  TTTTTTTT  TTTTTTTT  U
102  -E-----  -----  -----  E
      TUTTTTTT  TTTTTTTT  TTTTTTTT  U
103  --E-----  -----  -----  E
      TTUTTTTT  TTTTTTTT  TTTTTTTT  U
104  ---E-----  -----  -----  E
      TTTUTTTT  TTTTTTTT  TTTTTTTT  U
-----
*****
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- 46. Example Asymmetric VLAN Switch #1

Notice in the example above, each port has a unique VID.

To undo asymmetric VLANs for the Switch or stack, toggle to select <Clear> from **Set the devices to VLAN configuration:<>**, highlight APPLY and press **Enter**. When not using Asymmetric VLANs, you will need to set up VLANs manually.

## Configure Port Priority

Use the Setup Port Priority to configure priority settings for each port.

To configure port priority, highlight Priority on the Main Menu and press **Enter** to see the following screen:

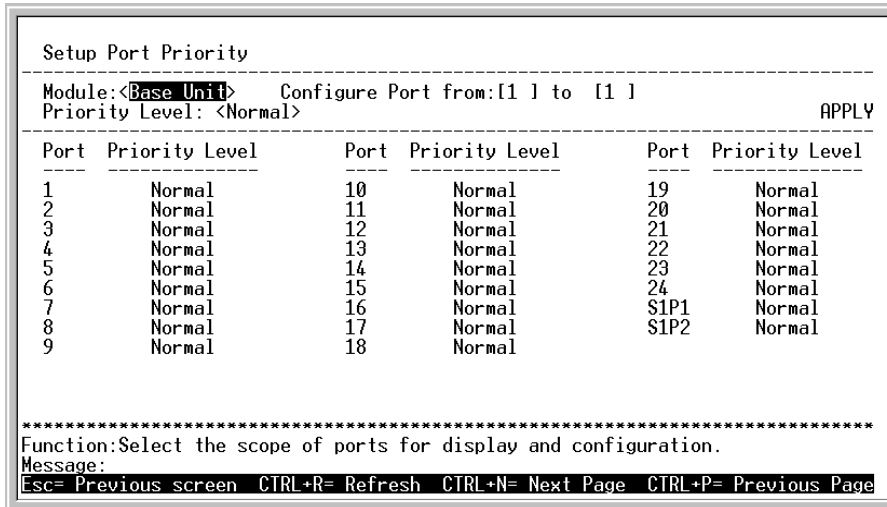


Figure 6- 47. Port Priority Screen

Use these fields to setup port priority:

- **Module** Toggle to select <Base Unit> or <Slot - 1>.
- **Configure Port from [ ] to [ ]** Type in the port number or sequential range of port numbers for which you wish to set priority.
- **Priority Level** Toggle to select priority level of the selected port(s), choose (listed lowest to highest) <Low>, <Med-L>, <Normal>, <Med-H> or <High>.

Highlight APPLY and press **Enter** to set the port priority. Use the Save Changes menu to save the settings to NV-RAM.

## Network Monitoring

The DHS-3224V provides extensive network monitoring capabilities.

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

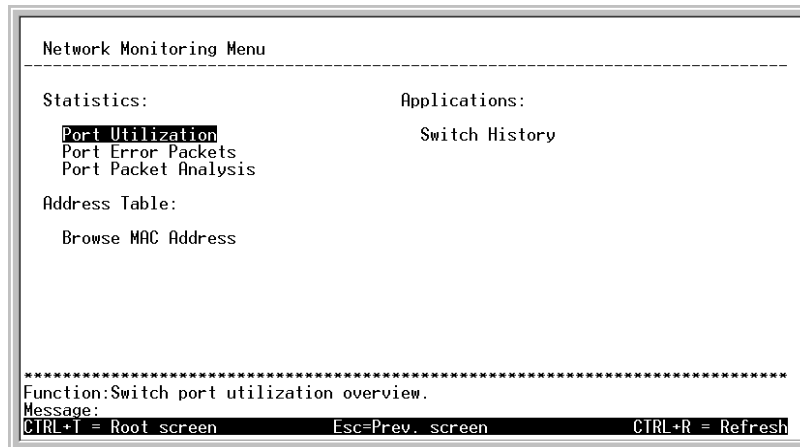


Figure 6- 48. Network Monitoring Menu

### 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**:

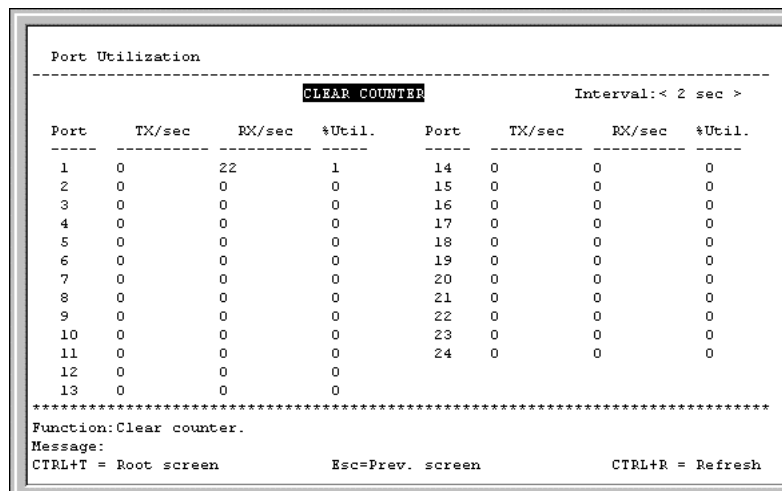


Figure 6- 49. Port Utilization Screen

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**:

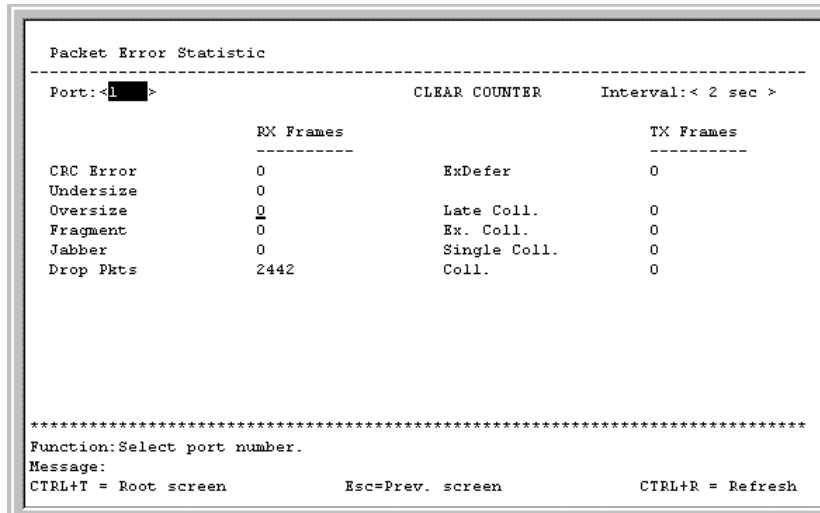


Figure 6- 50. Port Error Statistic Screen

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**:

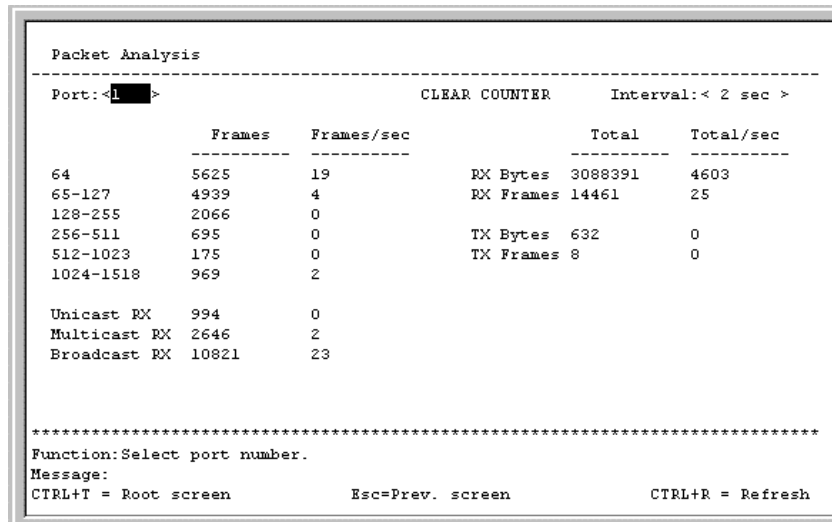


Figure 6- 51. Packet Analysis Table

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**:

```

Browse Address Table
-----
Browse By: <ALL > VLAN ID: [1 ] Total Addresses in Table: 192
MAC Address: [000000000000] BROWSE CLEAR ALL
-----
VID  MAC Address  Port  Status      VID  MAC Address  Port  Status
-----
1    0000819AF2F4  1     Dynamic     1    0020482D0A55  1     Dynamic
1    000102030400  1     Dynamic     1    0020485A70A2  1     Dynamic
1    000130FA5F00  1     Dynamic     1    00224488779B  1     Dynamic
1    0001969C0600  1     Dynamic     1    003326081100  1     Dynamic
1    00055DF93287  CPU   Self        1    004005254874  1     Dynamic
1    00055DF93616  1     Dynamic     1    0040052EAEDC  1     Dynamic
1    001002123457  1     Dynamic     1    004005400C85  1     Dynamic
1    00106F030FB1  1     Dynamic     1    00400541AFBF  1     Dynamic
1    001083CFA85E  1     Dynamic     1    00400551842F  1     Dynamic
1    001300000001  1     Dynamic     1    00400551E1DB  1     Dynamic
1    0020481A8547  1     Dynamic     1    00402647F56F  1     Dynamic
-----
*****
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
    
```

Figure 6- 52. 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**:

```

Switch History
-----
Seq.#  Date      Time      Log Text
-----
8      2000/00/00 00:00:00 Module 2, Port 1 Link Up
7      2000/00/00 00:00:00 Fan Working !
6      2000/00/00 00:00:00 Successful login through console.
5      2000/00/00 00:00:00 Cold Start
4      2000/00/00 00:00:00 Upgrade firmware from successfully.
3      2000/00/00 00:00:00 Successful login through console.
2      2000/00/00 00:00:00 Module 2, Port 1 Link Up
1      2000/00/00 00:00:00 Cold Start

- end (8 of 8)

*****
Function:View Switch Logs and Health Status
Message:
CTRL+N=Next Page  CTRL+P=Previous Page  B=Begin  E=End  C=Clear  CTRL+R=Refresh
    
```

Figure 6- 53. Switch History Screen

## System Utilities

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

```

Switch Utilities
-----

Switch Settings:

  Server IP Address: 10.43.10.1
  Switch IP Address: 10.24.22.3
    Subnet Mask: 255.0.0.0
  Gateway Router: 10.254.254.251

TFTP Services:                Others:

  Upgrade Firmware from TFTP Server    Ping Test
  Use Configuration File on TFTP Server
  Save Settings to TFTP Server
  Save History Log to TFTP Server

*****
Function:Upgrade firmware from TFTP server.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh
    
```

**Figure 6- 54. 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**.

```

Upgrade Firmware
-----

Server IP Address: [10.43.10.1 ]

Path\Filename: [c:\project\dhs-3224\runtime\image\dhs32]      APPLY

START

-----

*****
Function:Enter the Server IP address.
Message:
CTRL+T = Root screen          Esc=Prev. screen          CTRL+R = Refresh
    
```

**Figure 6- 55. Upgrade Firmware Screen**

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

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

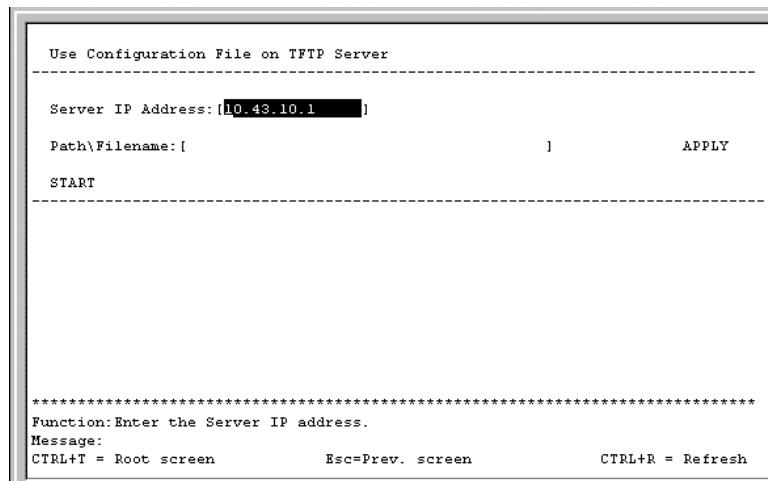
**Note:** The TFTP server must be on the same IP subnet as the Switch. Also, the TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages, or can be obtained as a separate program.

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 a Configuration File on TFTP Server** and press **Enter**.



**Figure 6- 56. 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.

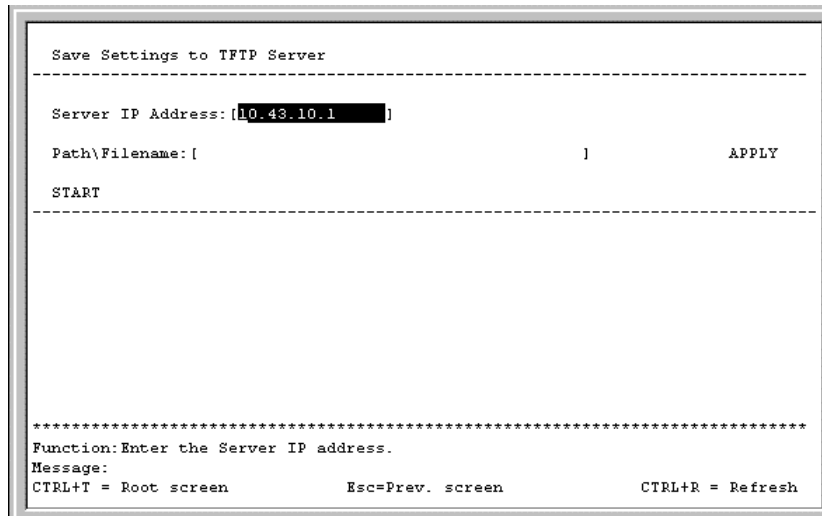
Highlight APPLY and press **Enter** to record the IP address of the TFTP server. Use **Save Changes** from the main menu to enter the address into NV-RAM

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



## Save Settings to TFTP Server

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

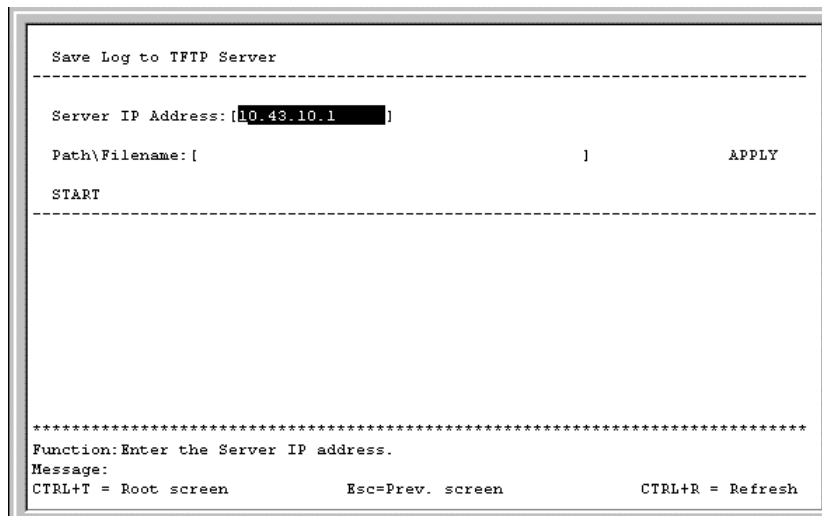


**Figure 6- 57. Save Settings to TFTP Server Screen**

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- 58. 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.

## Ping Test

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

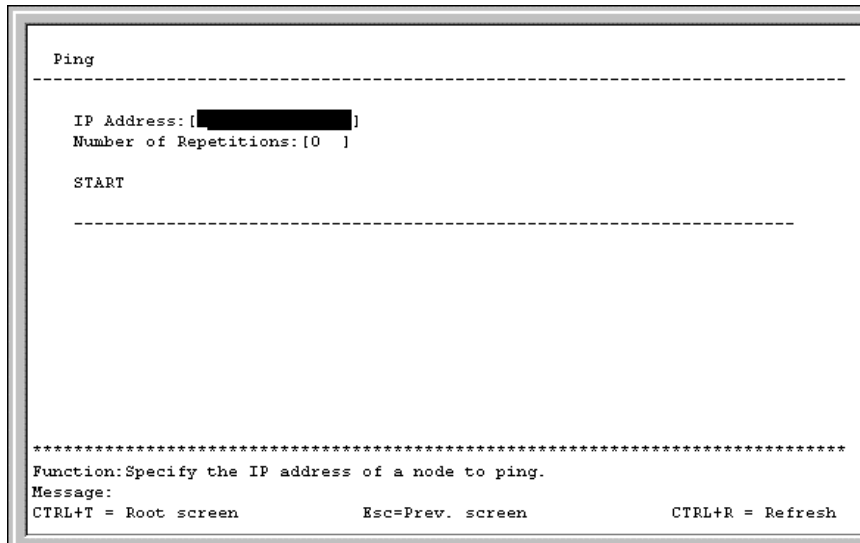


Figure 6- 59. Ping Test Screen

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.

## Local Loopback Test

To test the conduct a loopback test on the local loop, highlight **Local Loopback** and press **Enter**.

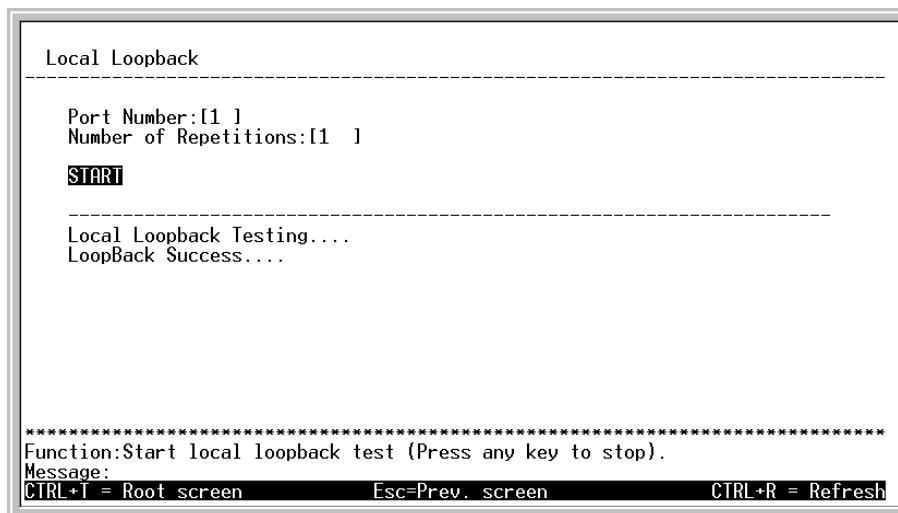
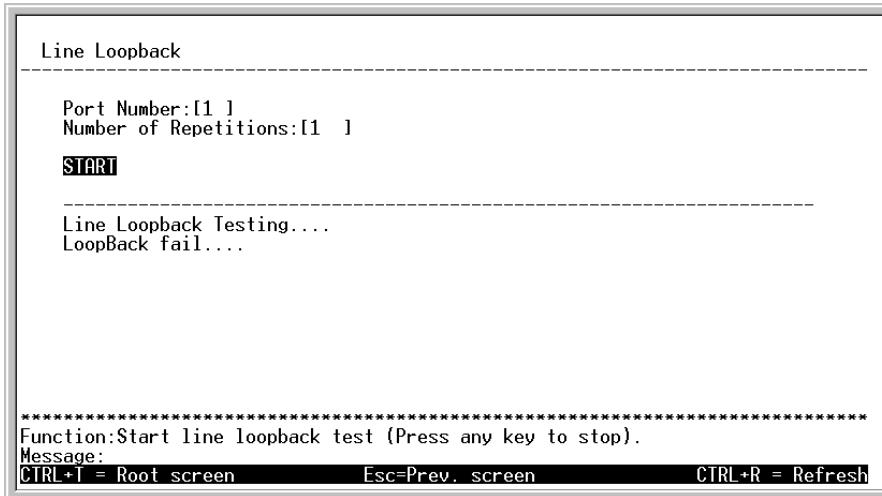


Figure 6- 60. Local Loopback Test Screen

Enter the port number to be tested and the number of repetitions for the test. Highlight **START** and press **Enter** to initiate the Local Loopback test. Success or failure of the test will be indicted upon its completion.

## Line Loopback Test

To test the conduct a loopback test on the line loop, highlight **Line Loopback** and press **Enter**.



**Figure 6- 61. Line Loopback Test Screen**

Enter the port number to be tested and the number of repetitions for the test. Highlight **START** and press **Enter** to initiate the Line Loopback test. Success or failure of the test will be indicated upon its completion.

---

## System Reboot

---

The DHS-3224V has several reboot options.

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

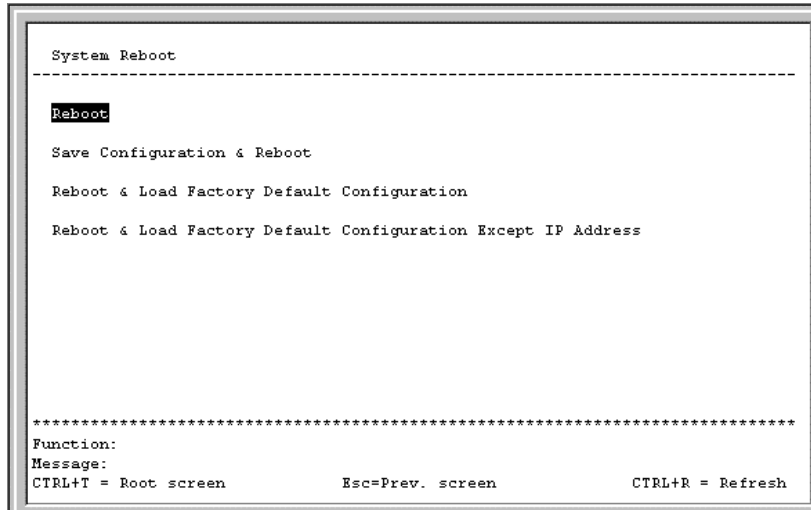
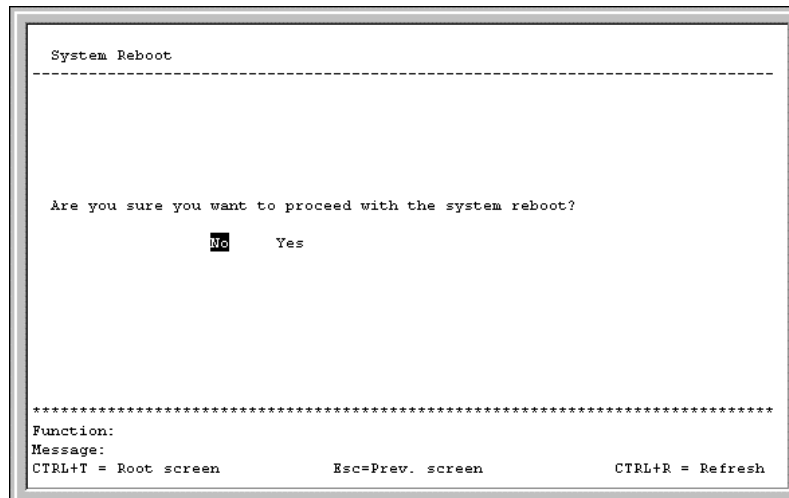


Figure 6- 62. System Reboot menu

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- 63. System Reboot Confirmation Screen**

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

## Logout

To logout from the console session, highlight Logout for the Main Menu and press **Enter**.



## ***Using the Web Management Software***

### **Introduction**

The DHS-3224V provides an embedded Web-based (HTML) interface, allowing users to manage the Switch from any remote station connected to the same network as the Switch. Using any common web browser, the administrator can communicate directly with the Switch using the HTTP protocol. The appearance of the your chosen browser window may differ from the screen captures that appear in this guide.

The Web-based management module and the Console program (and Telnet) 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 (see Chapter 6).

Since this chapter presents the same management functions as in Chapter 6, explanations of many management functions are abbreviated.

**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, 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).

## Log On to Web Manager

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

In the page that opens, click on **Login** to open the Web Manager.



Figure7- 1. Web Manager Login

Clicking on Login will bring up an authorization screen prompt. If you have not yet set up any user accounts (see *Setting Up User Accounts* in Chapter 6), there will not be any user name or password needed to login.

## Web Interface Components

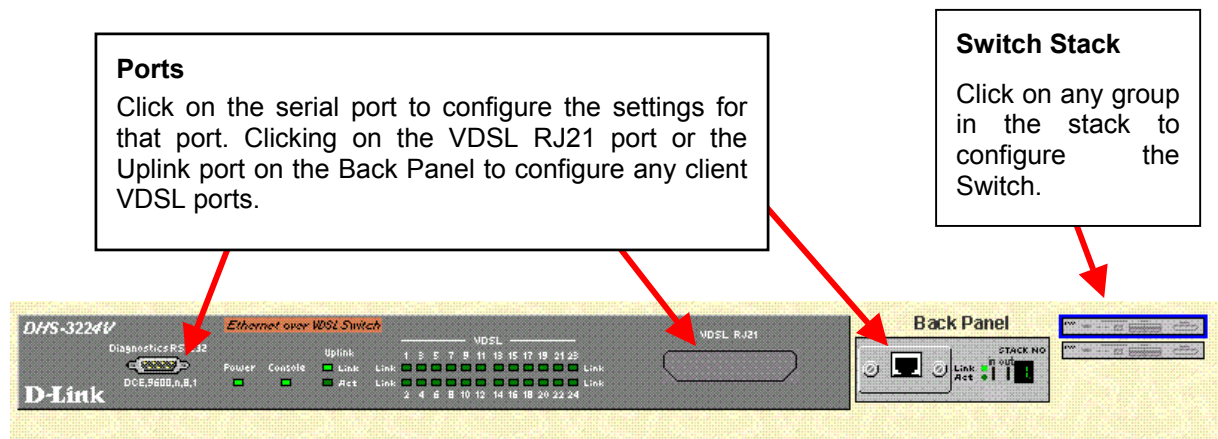


Figure7- 2. Top Section of Web Manager

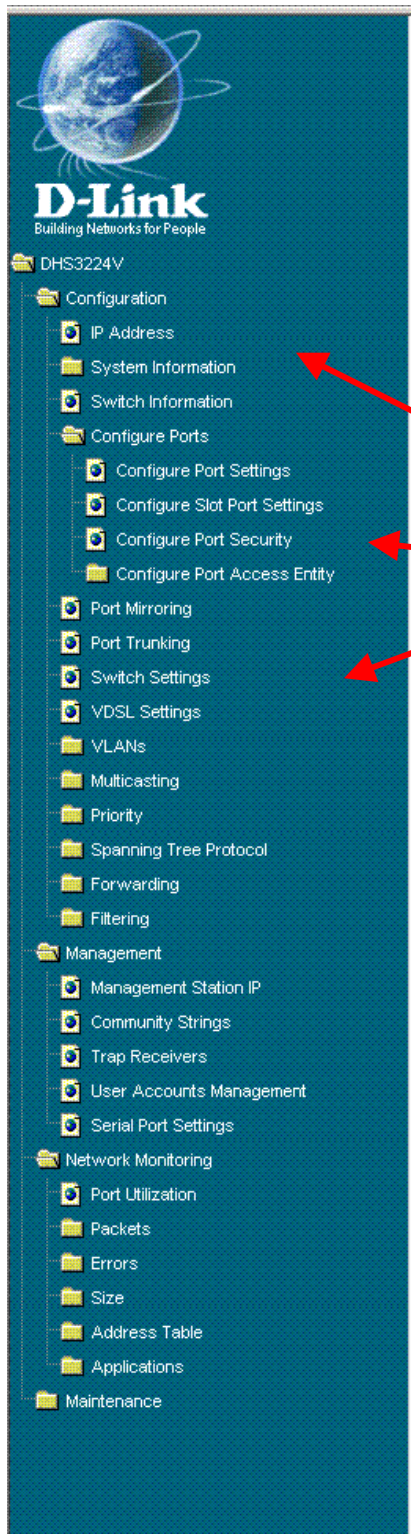
The top portion of the browser window presents virtual near real-time representations of the front and back panels of the Switch. The LEDs will appear lit up or dark, exactly as they appear on the Switch.

To configure serial port settings, click on the Diagnostics RS-232 port (for details see the section titled *Serial Port Settings*). To configure any of the subscriber ports, click on the Uplink port or the VDSL RJ21 port.

Click on any Switch in the stacked group (Unit 1 is on top) to view or configure that Switch.

### Accessing Menu Windows

To access the different menu windows, click on the folder or subfolder that contains the configuration menu you want. Each menu can be accessed by clicking on the corresponding button. The folders and subfolders are organized in the same fashion as the console interface.



Click on any folder to reveal the subfolders or hyperlinked menu buttons inside.

Figure7- 3. Web Manager Folders and Menus



## Switch Configuration

Click on the Configuration folder to reveal the menu buttons and subfolders used for basic and advanced configuration of the Switch.

### System Information

The first page you see when you successfully login displays the System Information menu.

System Information - Basic Settings	
Device Type	D-Link DHS-3224V Ethernet over VDSL Switch
Boot PROM Version	1.00-B02
Firmware Version	1.00-B49
Hardware Version	2A1
System Name	<input type="text" value="VDSL Switch Unit 4"/>
System Location	<input type="text" value="201 Park Ave. South B2-47 Wiring Closet"/>
System Contact	<input type="text" value="Ryan Sachs 212 555-5555"/>
<input type="button" value="Apply"/>	

Figure7- 4. First Menu – System Information

The first menu that appears after logging in displays the **System Information** menu. The System Information displays the switch type, which (if any) external modules are installed, and the Switch's **MAC Address**. In addition, the **Boot PROM**, **Firmware**, and **Hardware Version** numbers are shown. This information is helpful to keep track of updates and to obtain the Switch's MAC address for entry into other network device's address table – if necessary.

You can also enter **System Name**, **System Location**, and the name and telephone number of the administrator in the **System Contact**. It is recommended that the person responsible for the maintenance of the network system be listed here. Click on the *Apply* button to make the changes effective.

### System Time Setup

Use the **Setup System Time** menu to set the system clock.

Current System Time	
Date	2002 / 08 / 06
Time	<input type="text" value="15:21:27"/>
New System Time	
Date	20 <input type="text" value="00"/> / <input type="text" value="00"/> / <input type="text" value="00"/>
Time	<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/>
<input type="button" value="Apply"/>	

Figure7- 5. Setup System Time Menu

Enter the date and time, Click *Apply* to enter the system time information.

## IP Settings

View or change Switch IP settings.

IP Address	
<b>Current Settings</b>	
Get IP From	Manual
IP Address	10.41.44.90
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
Management VID	1
<b>New Settings</b>	
Get IP From	Manual
IP Address	10 . 41 . 44 . 90
Subnet Mask	255 . 0 . 0 . 0
Default Gateway	0 . 0 . 0 . 0
Management VID	1
Apply	

**Figure7- 6. IP Settings Window**

In the IP Settings window, read-only information includes the **Switch MAC Address** and the current IP settings (listed under **Current Settings**). Change IP settings under **New Settings**.

To change IP settings:

1. Select *Manual*, *BOOTP* or *DHCP* in the **Get IP From** menu.
2. If you are assigning IP settings manually, type in the IP settings for *IP Address*, *Subnet Mask* and *Default Gateway*.
3. Change the Management VLAN ID number in the **Management VID** box (default Management VID = 1).
4. Click the *Apply* button to make the changes effective.

## Switch Information

Use the Switch Information window to view basic information about the Switch or any Switch in a stacked group.

Switch Information(basic setting)	
Unit	1
MAC Address	00-05-5d-ed-85-2f
Ext. Module Type	10/100 TX 1 Port Module
Ext. Module Version	2A1
VDSL Patch File Version	0x0058
Fan Status	Good
Stacking Configuration	

**Figure7- 7. Switch Information**

For stacked Switch groups, select any Switch in the stack according to its number in the stack order (1 – 6) from the drop-down *Unit* menu.

The read-only information that can be viewed in the Stacking Information window is as follows:

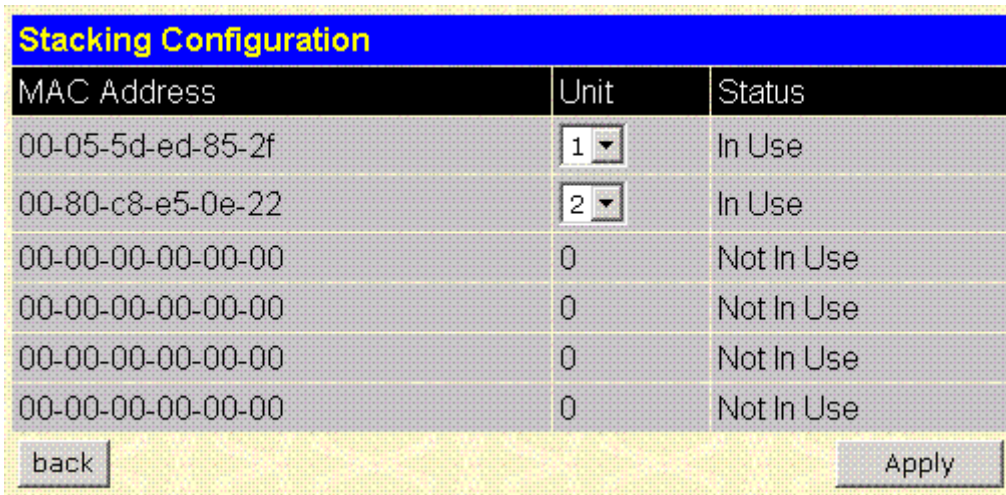
<b>MAC Address</b>	MAC address of the Switch
<b>Ext. Module Type</b>	Type of module (Extension Module) used for uplink to Ethernet backbone
<b>Ext. Module Version</b>	Version number of the Extension Module
<b>VDSL Patch File Version</b>	Version number of the VDSL Patch File
<b>Fan Status</b>	Current status of system fan, <i>Good</i> or <i>Fail</i>

**Note:** If the master Switch is changed, connect the Ethernet uplink to the new master.

To view or change the current configuration of the Switch stack hierarchy, click **Stacking Configuration** to view a new menu.

### Stacking Configuration

Use the Stacking Configuration menu to change or view the order (hierarchical order) of a stacked Switch group.



**Figure7- 8. Stacking Configuration Menu**

To change the stack order of the Switch stack, use the drop-down menu listed under *Unit* to select the desired order for this unit in the new hierarchy. Click *Apply* to force the new order. Remember that it is best to uplink to the master Switch, keep this in mind should you change the master (Unit 1) Switch.

Each Switch in the stack must be restarted in order to implement the change to the stack order. Once you have saved the new stack order configuration and rebooted all the Switches in the stack, the new logical stack order will be displayed in the Stacking Configuration screen in the order.

## Configure Ports

Use the Configure Ports menu to enable/disable and set the speed for any port.

Configure Port					
Port	DS/US Speed	VDSL Connection	Ethernet Connection	Rate Adapt	Edit
1	Mode 0	Link Down	Link Down	Default	More
2	Mode 0	Link Down	Link Down	Default	More
3	Mode 0	Link Down	Link Down	Default	More
4	Mode 0	Link Down	Link Down	Default	More
5	Mode 0	Link Down	Link Down	Default	More
6	Mode 0	Link Down	Link Down	Default	More
7	Mode 0	Link Down	Link Down	Default	More
8	Mode 0	Link Down	Link Down	Default	More
9	Mode 0	Link Down	Link Down	Default	More
10	Mode 0	Link Down	Link Down	Default	More
11	Mode 0	Link Down	Link Down	Default	More
12	Mode 0	Link Down	Link Down	Default	More
13	Mode 0	Link Down	Link Down	Default	More
14	Mode 0	Link Down	Link Down	Default	More
15	Mode 0	Link Down	Link Down	Default	More
16	Mode 0	Link Down	Link Down	Default	More
17	Mode 0	Link Down	Link Down	Default	More
18	Mode 0	Link Down	Link Down	Default	More
19	Mode 0	Link Down	Link Down	Default	More
20	Mode 0	Link Down	Link Down	Default	More
21	Mode 0	Link Down	Link Down	Default	More
22	Mode 0	Link Down	Link Down	Default	More
23	Mode 0	Link Down	Link Down	Default	More
24	Mode 0	Link Down	Link Down	Default	More

Figure7- 9. Configure Port Table

The information listed for each port is summarized in the table below. To configure any individual port settings, click on the *More* button for that port and a new menu appears. The new menu allows you to configure any port or range of consecutive ports on the Switch.

<b>Speed</b>	4M/1M, 5M, 10M or 15M
<b>VDSL Connection</b>	Upstream Speed/ Downstream Speed/ Symmetry Condition
<b>Ethernet Connection</b>	Connection Speed/Duplex Mode/Flow Control Method.
<b>Rate Adaptive</b>	The VDSL Rate Adaptive feature automatically senses line condition and adjusts DS/US speeds if a set rate cannot be maintained. The default setting will set speed to Mode 0 when a rate can no longer be supported. Optimum setting sets speed to Mode 0 but then tests raises the DS/US speed incrementally to achieve the best performance level.

Clicking on the *More* button for any port will bring up the Configure Port menu for that port.

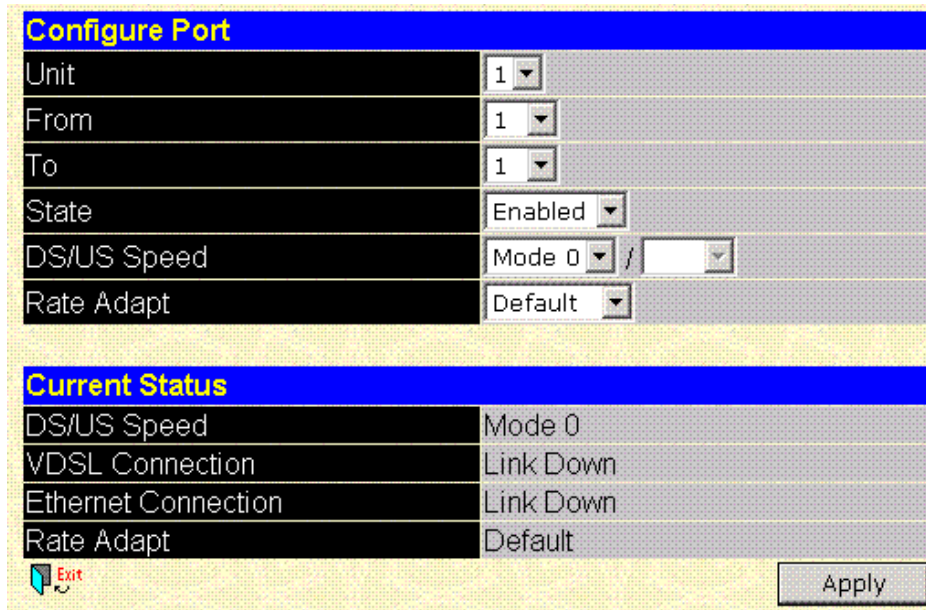


Figure7- 10. Configure Port Settings Window

For ports 1 – 24, configure the ports by selecting options described below:

Select the **Unit** using the drop-down menu and choose ports with the **From** and **To** drop-down menus.

Use **State** to enable or disable the selected port(s).

**DS/US Speed** can use any combination of download and upload speed. Default setting is *Mode 0*. Mode 0 has a DS/US Speed set to 4M/ 1M. If you select any speed except Mode 0, you can change the DS and US speed. Speed for both DS and US may be changed to 512K, 1M, 2M, 3M, ... up to 15M using the drop-down menus. Any changes to port speed must take into account the line distance to the CPE. VDSL Settings may also require adjustment (see 65 for VDSL Settings).

Set **Rate Adapt** to *Default*, *Optimum*, and *Disabled* with the drop-down menu.

Click APPLY to make the change effective.

### Configure Slot Module Port

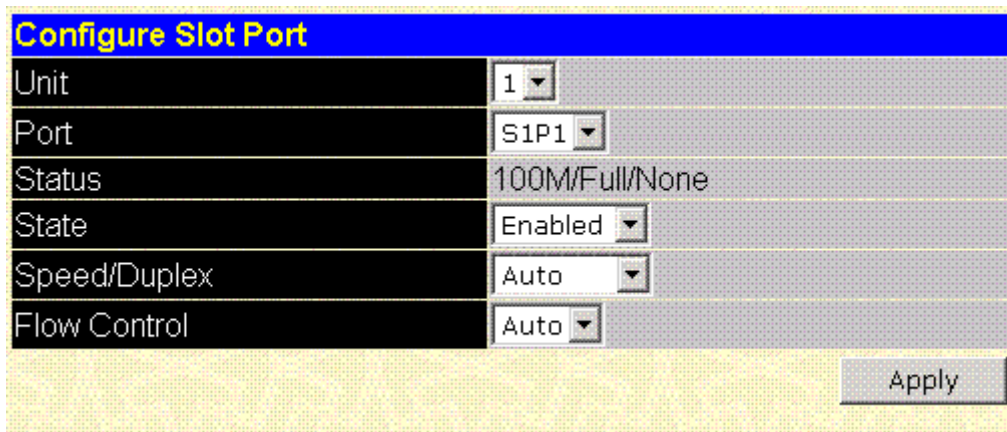


Figure7- 11. Configure Slot Module Port Window

The Configure Slot Port menu is used to configure the uplink port. Use the **State** drop-down menu to *Enable* or *Disable* the slot port. Set speed/duplex in the **Speed/Duplex** drop-down, choose *Auto*, *10/Half*, *10/Full*, *100/Half* or *100/Full*. The default setting is Auto. The Auto setting adjusts automatically according to the speed/duplex status of the remote connection to the slot port. **Flow Control** settings are determined by the Speed/Duplex

settings and can not be enabled or disabled except in either 10/Full or 100/Full mode. For Speed/Duplex settings 10/Half or 100/Half, flow control is set to *Back Pressure* mode and can not be changed.

### Configure Port Security

Configure Port Security			
Port	Lock	No. of MAC	Edit
1	Disabled	-	More
2	Disabled	-	More
3	Disabled	-	More
4	Disabled	-	More
5	Disabled	-	More
6	Disabled	-	More
7	Disabled	-	More
8	Disabled	-	More
9	Disabled	-	More
10	Disabled	-	More
11	Disabled	-	More
12	Disabled	-	More
13	Disabled	-	More
14	Disabled	-	More
15	Disabled	-	More
16	Disabled	-	More
17	Disabled	-	More
18	Disabled	-	More
19	Disabled	-	More
20	Disabled	-	More
21	Disabled	-	More
22	Disabled	-	More
23	Disabled	-	More
24	Disabled	-	More
S1P1	Disabled	-	More

Figure7- 12. Configure Port Security Window

Port security status listed in the Configure Port Security window is summarized below. Configure port security for any port by clicking on the *More* button, a new menu appears. Use the new menu (pictured in Figure 7-11 below) to *Enable* or *Disable* the Port Lock and choose the number of MAC addresses allowed for the port.

<b>Lock</b>	Enabled or Disabled
<b>No. of MAC</b>	Number of MAC addresses allowed for the port

Configure Port Security	
Unit	1
From	1
To	1
Lock	Disabled
No. of MAC	0

Current Status	
Lock	Disabled
No. of MAC	-

Exit Apply

**Figure7- 13. Configure Individual Port Security Menu**

Selecting *Enabled* activates the drop-down menu that lets you select a maximum number of MAC addresses allowed for the port. From 0 to 16 MAC addresses can be allowed when the lock is enabled.

## PAE System Control

The Port Access Entity Control section allows you to use the Switch's 802.1X port-based authentication feature.

### Port Authenticating Settings

802.1X Capability Settings				
Unit	From	To	Capability	Apply
1	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
S1P1	None

Figure7- 14. 802.1X Capability Settings window

To set up the Switch's 802.1X port-based authentication, select the **Unit** then 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)

Initialize Port						
Unit	From	To	Apply			
1	Port 1	Port 1	Apply			

Initialize Port Table						
Port	AuthState	BackendState	AdmDir	OprDir	PortStatus	PortControl

Figure7- 15. 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**.

### Reauthenticate Ports(s)

Reauthenticate Port						
unit	From	To	Apply			
1	Port 1	Port 1	Apply			

Reauthenticate Port Table						
Port	AuthState	BackendState	AdmDir	OprDir	PortStatus	PortControl

Figure7- 16. 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**.

## Configure Authenticator

802.1X Authenticator Settings						
unit	From	To	AdmDir	PortControl	TxPeriod	
1	Port 1	Port 1	both	forceUnauthorized	30	
QuietPeriod	SuppTimeout	ServerTimeout	MaxReq	ReAuthPeriod	ReAuth	Apply
60	30	30	2	3600	Disabled	Apply

802.1X Authenticator Settings									
Port	AdmDir	Ctrl Stat	TxPeriod	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

Figure7- 17. 802.1X Authenticator Settings window

This window allows you to set the following features:

<b>Unit</b>	Select the unit in the stack order to configure.
<b>From [ ] To [ ]</b>	Select the port or ports to be set.
<b>AdmDir</b>	Sets the administrative-controlled direction to either <i>in</i> or <i>both</i> . If <i>in</i> is selected, control is only exerted over incoming traffic through the port you selected in the first field. If <i>both</i> is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
<b>PortControl</b>	This allows you to control the port authorization state. Select <i>forceAuthorized</i> 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 <i>forceUnauthorized</i> 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 <i>auto</i> . 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. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address.
<b>TxPeriod</b>	This sets the period of time for the authenticator PAE state machine.
<b>QuietPeriod</b>	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.
<b>SuppTimeout</b>	This sets the port's suppTimeout for the Backend Authentication state machine.
<b>ServerTimeout*</b>	This sets the port's serverTimeout for the Backend Authentication state machine.
<b>MaxReq</b>	Set this for the Backend Authentication state machine.
<b>ReAuthPeriod</b>	Set this for the Reauthentication Timer state machine.
<b>ReAuth</b>	Toggle the port's re-authenticating control between <i>Enabled</i> and <i>Disabled</i> .

**\*Note:** The *ServerTimeout* value must be set to a value that is less than the *Radius Timeout* and *Radius Maximum Retransmit* settings (see Configure General Radius Server Setting)

## 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

Figure7- 18. General Radius Server Setting window

This window allows you to set the following features:

<b>AuthProtocol</b>	Toggle between the authentication protocol options: <i>Radius Server(Support EAP)</i> and <i>Local</i> .
<b>Radius Dead Time</b>	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.
<b>Radius Time Out*</b>	This specifies the number of seconds NAS waits for a reply to a RADIUS request before transmitting the request.
<b>Radius Maximum Retransmit*</b>	This specifies the number of times NAS transmits each RADIUS request to the server before giving up.
<b>Accounting Method</b>	To use a RADIUS Server, toggle from <i>None</i> to <i>Radius Server</i> .
<b>Accounting Mode</b>	Select the desired method: <i>Start and Stop</i> , <i>Stop only</i> , or <i>None</i> .

**\*Note:** The *ServerTimeout* value must be set to a value that is less than the *Radius Timeout* and *Radius Maximum Retransmit* settings (see 802.1X Authenticator Settings)

## Authentic Radius Server

**Authentic Radius Server Setting**

<b>Succession</b>	First <input type="button" value="v"/>
<b>Radius Server</b>	<input type="text" value="0.0.0.0"/>
<b>Authentic Port</b>	<input type="text" value="1"/>
<b>Accounting Port</b>	<input type="text" value="1"/>
<b>Key</b>	<input type="text"/>
<b>Confirm Key</b>	<input type="text"/>
<b>Accounting Method</b>	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

**Figure7- 19. Authentic Radius Server Setting window**

This window allows you to set the following features:

<b>Succession</b>	Choose the desired RADIUS server to configure: <i>First</i> , <i>Second</i> or <i>Third</i> .
<b>Radius Server</b>	Set the RADIUS server IP.
<b>Authentic Port</b>	Set the RADIUS account server(s) UDP port. The default is <i>1812</i> .
<b>Accounting Port</b>	Set the RADIUS account server(s) UDP port. The default is <i>1813</i> .
<b>Key</b>	Set the key the same as that of the RADIUS server.
<b>Confirm Key</b>	Confirm the shared key is the same as that of the RADIUS server.
<b>Accounting Method</b>	This allows you to set the RADIUS server as <i>Valid</i> or <i>Invalid</i> .

## Local User

**Local Users Setting**

User ID	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Status	Valid

Apply

Note: The "Password" and "Confirm Password" should be the same, or the setup will be invalid.

The Local User:

Figure7- 20. Local Users Setting window

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

## Port Mirroring

**Port Mirroring**

Source Unit	1
Source Port	Port 1
Source Direction	Ingress & Egress
Target Unit	1
Target Port	Port 9
Status	Disabled

Apply

Note(1): The "Source Port" and "Target Port" should be different, or the setup will be invalid.

Note(2): Target port should not be port lock enabled port.

Note(3): Target port should not be 802.1x enabled port.

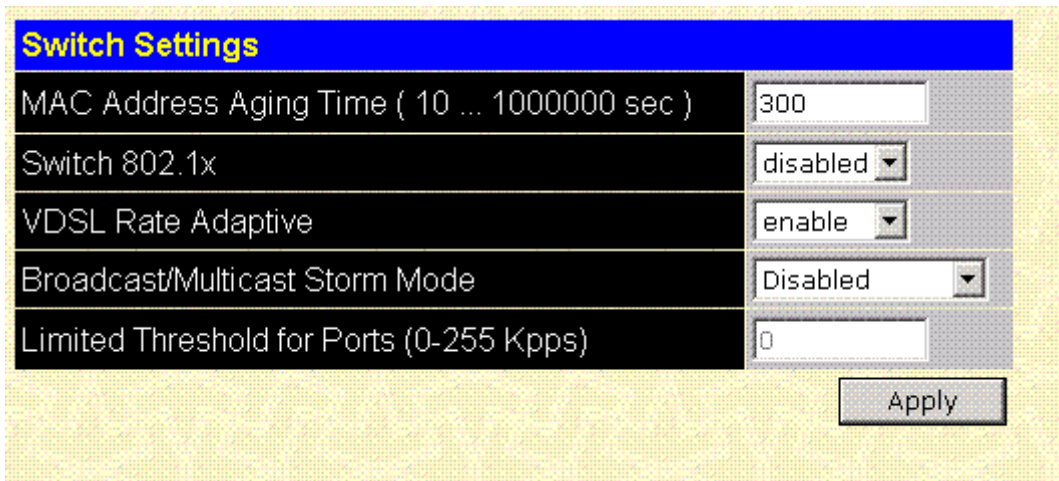
Figure7- 21. Port Mirroring window

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 *Ingress & Egress* and change the *Status* pull-down menu to *Enabled*. Finally, click **Apply** to let the changes take effect.

**Note:** You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port 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.

## Switch Settings



**Figure7- 22. Switch Settings**

Use the Switch Settings menu to change the following fields:

<b>MAC Address Aging Time (sec):[300 ] *</b>	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.
<b>Switch 802.1x</b>	This allows you to set 802.1x Port Based Network Access for the whole Switch.
<b>VDSL Rate Adaptive</b>	This must be enabled if you use the Rate Adaptive feature when you configure port settings.
<b>Broadcast / Multicast Storm Mode</b>	Select Enabled or Disabled to globally enable or disable the Switch's reaction to Broadcast storms, triggered at the threshold set below.
<b>Limited Threshold for Ports</b>	This is the number of Broadcast/Multicast packets in Kbps received by the switch - on one of the base ports - that will trigger the switch's reaction to a Broadcast/Multicast storm.

**\*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 to soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table.

## VDSL Settings

DS Tx Power can be changed on a per port basis. However, the settings for all ports on each individual Switch should be the same.

- IMPORTANT:** Before changing the default DS Tx Power setting, consider the following:
1. National or local telecommunications regulations may limit the range of settings that can be used.
  2. Each Switch unit should use the same settings for all ports on the Switch.
  3. Consider the effects of changing the DS Tx Power on upstream and downstream SNR.

The screenshot shows the 'VDSL Setting' menu. At the top, there are dropdown menus for 'Unit' (set to 1), 'From' (set to port 1), and 'To' (set to port 1). A text input field for 'DS Tx Power' contains '-58.00', and an 'Apply' button is next to it. Below this is a table titled 'VDSL Setting of Unit 1' with 24 rows and 5 columns: Port, US Tx Power, DS Tx Power, US SNR, and DS SNR. The DS Tx Power column shows '-58.00' for every port from 1 to 24.

Port	US Tx Power	DS Tx Power	US SNR	DS SNR
1		-58.00		
2		-58.00		
3		-58.00		
4		-58.00		
5		-58.00		
6		-58.00		
7		-58.00		
8		-58.00		
9		-58.00		
10		-58.00		
11		-58.00		
12		-58.00		
13		-58.00		
14		-58.00		
15		-58.00		
16		-58.00		
17		-58.00		
18		-58.00		
19		-58.00		
20		-58.00		
21		-58.00		
22		-58.00		
23		-58.00		
24		-58.00		

Figure7- 23. VDSL Settings Menu

Choose the Switch unit and port from the drop-down menus and type in a value for the **DS Tx Power** (Downstream Transmitting Power). The DS Tx Power must be within the range -90 to -55 dBm/Hz.



## Configure 802.1Q Static VLANs

The following figures and tables describe how to set up 802.1Q VLANs on the switch.

802.1Q Static VLANs			
VLAN ID (VID)	VLAN Name	New	Delete
1	DEFAULT_VLAN	More	X
2	PH-1 AAA Air	More	X
3	PH-2 Phil	More	X

Figure7- 24. 802.1Q Static VLANs Screen

The Static VLANs menu lists existing VLANs by their VLAN ID (VID) and by name. To create a new VLAN, click on the *New* button in the header row of the table. To edit an existing VLAN, click on the *More* button of the VLAN you want to edit. To eliminate an entire VLAN, click on the “X” button for the VLAN you wish to delete.

## Add a Static 802.1Q VLAN

The following figure and table describe how to add an 802.1Q VLAN on the switch.

802.1Q Static VLANs Entry Settings -- Add

VLAN ID (VID): 4

VLAN Name: PH-4 Fly

Unit: 1

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	S1P1
Tag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
None	<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"/>	<input type="checkbox"/>
Egress	<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"/>	<input type="checkbox"/>

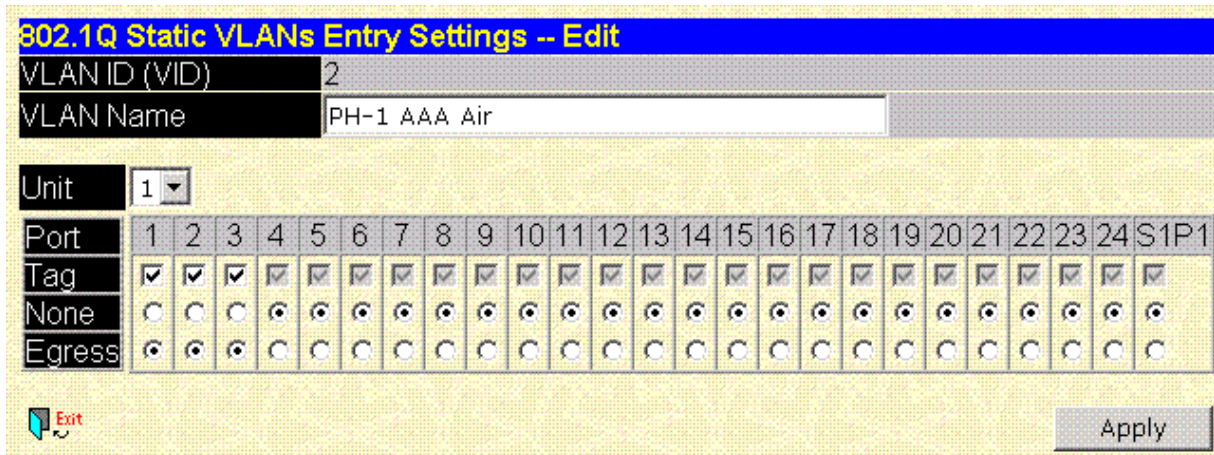
Exit Apply

Figure7- 25. 802.1Q Static VLANs Entry Settings – Add Screen

<b>VID</b>	The VLAN ID of the VLAN that is being created.
<b>VLAN Name</b>	The name of the VLAN that is being created.
<b>Port</b>	Corresponds to the ports that will be members of the VLAN.
<b>Tag</b>	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
<b>None</b>	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
<b>Egress</b>	Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.
<b>Forbidden</b>	Specifies the port as not being a static member of the VLAN, and as being forbidden from joining the VLAN dynamically.

## Edit 802.1Q VLANs

The following figure and table describe how to edit an existing 802.1Q VLAN entry on the switch.



**Figure7- 26. 802.1Q Static VLANs Entry Settings – Edit Screen**

The Static VLANs Edit screen presents the current configuration of the VLAN. Use this screen to change settings for the VLAN as described in the table below.

<b>VLAN ID (VID)</b>	The VLAN ID of the VLAN to be edited. For editing, VLANs are identified by name.
<b>VLAN Name</b>	The name of the VLAN to be edited.
<b>Port</b>	A list of the ports that are static members of the currently selected VLAN.
<b>Tag</b>	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
<b>None</b>	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
<b>Egress</b>	Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.
<b>Forbidden</b>	Specifies the port as not being a static member of the VLAN, and as being forbidden from joining the VLAN dynamically.

### 802.1Q Port Settings

Open the 802.1Q Port Settings menu and click on the first button, Port VLAN ID to assign new PVID as described below.

#### Port VLAN ID (PVID)

The following figure and table describe how to configure the PVID for the switch.

Port	PVID	Port	PVID
1	1	14	1
2	1	15	1
3	1	16	1
4	1	17	1
5	1	18	1
6	1	19	1
7	1	20	1
8	1	21	1
9	1	22	1
10	1	23	1
11	1	24	1
12	1	S1P1	1
13	1		

Apply

Figure7- 27. Port VLAN ID (PVID) Screen

<b>Port VLAN ID</b>	<p>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.</p> <p>If a packet is received by the port, 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.</p>
<b>Port</b>	Shows the current PVID assignment for each port. The switch's default is to assign all ports to the Default_VLAN with a VID of 1.

**Port Ingress Filter**

The following figure and table describe how to configure a Port Ingress Filter on the switch.

Port Ingress Filter			
Port	Ingress Filter	Port	Ingress Filter
1	Disabled	14	Disabled
2	Disabled	15	Disabled
3	Disabled	16	Disabled
4	Disabled	17	Disabled
5	Disabled	18	Disabled
6	Disabled	19	Disabled
7	Disabled	20	Disabled
8	Disabled	21	Disabled
9	Disabled	22	Disabled
10	Disabled	23	Disabled
11	Disabled	24	Disabled
12	Disabled	S1P1	Disabled
13	Disabled		

Apply

**Figure7- 28. Port Ingress Filter Screen**

<b>Port</b>	The number of the port for which ingress filtering is to be Enabled or Disabled.
<b>Ingress Filter</b>	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.

## Asymmetric VLANs

Use Asymmetric VLANs to assign a unique PVID to each port on the Switch. This may be a more convenient way to assign VLANs if you want to give each client port its own separate VLAN. For multiple Switch installations, the uplink ports belong to VLAN 1 (PVID = 1).

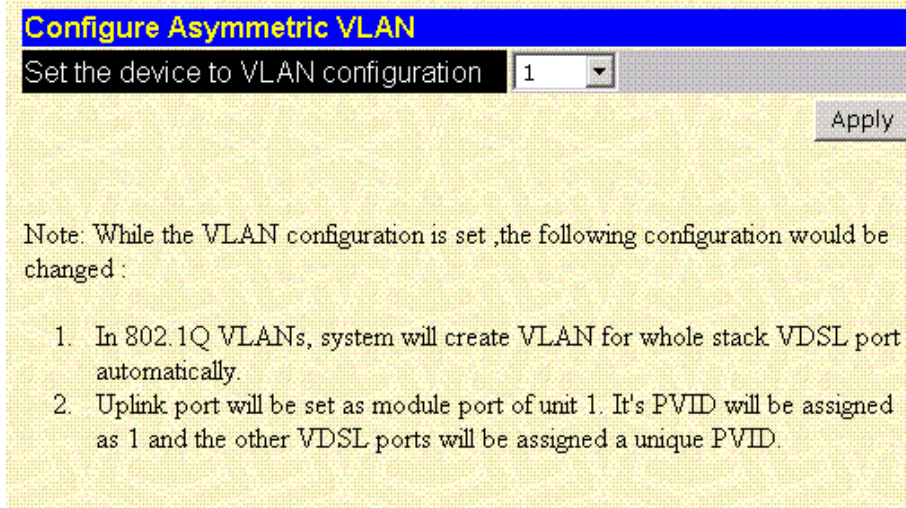


Figure7- 29. Configure Asymmetric VLANs Menu

Select the stack order number of the Switch from the drop-down menu. To enable Asymmetric VLANs for the selected Switch, click on APPLY.

## Multicasting Options

Multicasting functions can be customized for improve network performance using the menus available in the Multicasting folder.

### Group Address Filtering



Figure7- 30. Group Address Filtering Menu

The Group Address Filter is used to customize filtering and forwarding of multicast packets for the entire Switch. A multicast packet is “registered” if its source address is listed in the multicast table. To change the Group Address Filter Mode, select the desired setting from the **Group Address Filter Mode:** drop-down menu. The options are summarized below:

<b>Filter All Unregistered</b>	Filters all unregistered multicast packets.
<b>Forward All</b>	Forwards all multicast packets according to VLAN assignment.
<b>Forward All Unregistered</b>	Forwards all unregistered multicast packets.

## Multicast Forwarding

The following figure and table describe how to set up Multicast forwarding on the switch. Open the Multicasting folder and click on the 802.1Q Multicast Forwarding button to see the entry screen below:

Figure7- 31. Setup IEEE 802.1Q Multicast Forwarding Screen

Use the Multicast Forwarding Screen to define the following parameters:

<b>MAC Address</b>	The MAC address of the static source of multicast packets.
<b>VID</b>	The VLAN ID of the VLAN the above MAC address belongs to.
<b>PortMap / State</b>	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are; None – no restrictions on the port dynamically joining the multicast group, Egress – the port is a static member of the multicast group, and Forbidden – the port is restricted from joining the multicast group dynamically. For example, if None is chosen, then an end station attached to the port can join the multicast group using GMRP.

## IGMP Snooping

When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa.

Figure7- 32. IGMP Snooping Settings Screen

The user-changeable parameters for IGMP Snooping are as follows:

<b>IGMP Snooping State</b>	Select Enabled to implement IGMP Snooping.
<b>Querier State</b>	Choose V1 Querier for version 1 querier, V2 Querier for version 2 querier, or Non-Querier.
<b>Robustness Variable</b>	This entry field allows an entry of 2 to 255. Adjust this variable according to expected packet loss. If packet loss is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss.
<b>Query Interval</b>	The Query field allows an entry between 1 and 9,999 seconds and defines the time between transmitting IGMP queries.
<b>Max Response</b>	The Max-Response field allows an entry between 1 and 254 and defines the maximum time allowed before sending a response report to a query measured in units of 1/10 of a second. This is used to adjust the "leave latency", the time interval between the moment the last host leaves a group and when the routing protocol is notified there are no more members.
<b>Age-out Timer</b>	Displays the time the Switch waits between IGMP queries

## Priority

Use the Setup Port Priority menu to change priority settings for any port.

Unit	From	To	Priority Level	Apply
1	Port 1	Port 1	Normal	Apply

Entries	
Port	Priority Level
1	Normal
2	Normal
3	Normal
4	Normal
5	Normal
6	Normal
7	Normal
8	Normal
9	Normal
10	Normal
11	Normal
12	Normal
13	Normal
14	Normal
15	Normal
16	Normal
17	Normal
18	Normal
19	Normal
20	Normal
21	Normal
22	Normal
23	Normal
24	Normal
S1P1	Normal

**Figure7- 33. Setup Port Priority**

Use these fields to setup port priority under *Modify an Entry*:

<b>Port</b>	Choose the port for which you will change priority settings.
<b>Priority Level</b>	Choose the level of priority for the port; select (listed lowest to highest) <i>Low, Med-L, Normal, Med-H</i> or <i>High</i> .

Click on the *Apply* button to make the changes effective.



## Spanning Tree Protocol Configuration

The following figures and tables describe the configuration of the Spanning Tree Protocol (STP) on the switch.

**STP Switch Settings**

Spanning Tree Protocol	Disabled
Max Age: (6 .. 40 sec)	20
Hello Time: (1 .. 10 sec)	2
Forward Delay: (4 .. 30 sec)	15
Bridge Priority: (0 .. 65535)	32768

Apply

**The above values must conform to this formula:**  
 $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

Figure7- 34. STP Switch Settings Menu

Set the parameters listed below in the STP Switch Settings menu.

<b>Spanning Tree Protocol</b>	Allows the STP to be globally Enabled or Disabled on the switch. Default = Enabled.
<b>Max Age</b>	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or $[2 \times (\text{Hello Time} + 1)]$ . The maximum value is the lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$ . Default = 20 Default = 20
<b>Hello Time</b>	The time interval (in seconds) at which the root device transmits a configuration message. Default = 2
<b>Forward Delay</b>	The maximum time (in seconds) the root device will wait before changing states (i.e., from the listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward packets. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. Maximum value is 30 Minimum value is the higher of 4 or $[(\text{Max. Age} / 2) + 1]$ Default = 15
<b>Bridge Priority</b>	Device priority used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. The lower the numeric value, the higher the priority. If all devices have the same priority, the device with the lowest MAC address will become the root device. Range 0 to 65535. Default = 32,768

## Port Spanning Tree

STP Port Settings							
Port	Cost	Priority	Status	Port	Cost	Priority	Status
1	250	128	Disabled	14	250	128	Disabled
2	250	128	Disabled	15	250	128	Disabled
3	250	128	Disabled	16	250	128	Disabled
4	250	128	Disabled	17	250	128	Disabled
5	250	128	Disabled	18	250	128	Disabled
6	250	128	Disabled	19	250	128	Disabled
7	250	128	Disabled	20	250	128	Disabled
8	250	128	Disabled	21	250	128	Disabled
9	250	128	Disabled	22	250	128	Disabled
10	250	128	Disabled	23	250	128	Disabled
11	250	128	Disabled	24	250	128	Disabled
12	250	128	Disabled	S1P1	19	128	Forwarding
13	250	128	Disabled				

Apply

**Figure7- 35. Spanning Tree Port Settings**

The Port Group STP parameters that can be configured are:

<b>Port Cost</b>	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.
<b>Priority</b>	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.

## MAC Forwarding

Use the following screen to setup static unicast forwarding on the switch.

Figure7- 36. MAC Address Forwarding Entry Screen

To add an entry, define the following parameters in the **Add an Entry** field:

<b>MAC Address</b>	The MAC address to which packets will be statically forwarded.
<b>VID</b>	The VLAN ID number of the VLAN to which the above MAC address belongs.
<b>PortMap</b>	Allows the designation of the port on which the above MAC address resides.

Use the **Entries** field to select any existing entry and remove it from the forwarding table. Select the MAC address you want to remove, and click the *Remove* button.

## MAC Filtering

Use the following screen to setup static unicast forwarding on the switch.

Figure7- 37. MAC Address Filtering Setup Screen

To add an entry, define the following parameters in the **Add an Entry** field:

<b>MAC Address</b>	The MAC address to which packets will be statically forwarded.
<b>VID</b>	The VLAN ID number of the VLAN to which the above MAC address belongs.
<b>State</b>	Choose Dst, Src or Either from the drop-down menu to filter packets based on destination, source or either MAC address.

Use the **Entries** field below to select any existing entry and remove it from the forwarding table. Select the MAC address you want to remove, and click the *Remove* button.

## Management

The Management folder is used to define parameters for SNMP agents.

### Management Station IP Settings

Use the Management Station IP Settings screen to choose one to three management stations.

Figure7- 38. Management Station IP Address Screen

Use the Management Station IP Settings to select up to three management stations used to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address in the area provided and click on the *Apply* button.

**Note:** If you are not currently running the web manager from one of the IP addresses defined in the Management Station IP Settings screen, you will lose access to the web manager when you click on Apply.

## Community Strings

Use the Community Strings menu to define up to four community strings. Community strings are used to verify who can receive SNMP information from the switch.

Community String	Access Right	Status
public	Read-Only	Valid
private	Read-Write	Valid
	Read-Only	Invalid
	Read-Only	Invalid

Figure7- 39. Community Strings Menu

Type in the Community String in any of the four entry fields. Use the drop-down menu to define the Access Right and Status of the corresponding string. For the Access Right, select Read-Write or Read Only. Under Status, choose Valid to enable the string or Invalid to disable it.

## Trap Receivers

The following menu allows the user to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 4 trap managers may be entered.

SNMP Trap Manager Configuration		
Trap Receiving Station	Community String	Status
0 . 0 . 0 . 0		Disabled ▾
0 . 0 . 0 . 0		Disabled ▾
0 . 0 . 0 . 0		Disabled ▾
0 . 0 . 0 . 0		Disabled ▾

Apply

Figure7- 40. Trap Receivers Menu

To set up trap receivers, define the following:

<b>Trap Receiving Station</b>	Type in the IP address of the trap recipient, i.e. the IP address of the management station that will receive traps generated by the switch.
<b>Community String</b>	Type in a string of up to 20 characters used for authentication of users wanting to receive traps from the switch's SNMP agent.
<b>Status</b>	Choose Enabled or Disabled for the string. This is used to temporarily limit the receipt of traps generated by the switch.

## User Accounts

Use the User Accounts Control Table to control user privileges.

User Accounts Control Table		
User Name	Access Right	New
eviljulius	Root	More
mybrainhurts	User	More
tonyisagod	User+	More

Figure7- 41. User Accounts Control Table

To add a new user, click on the *New* button. To modify or delete an existing user, click on the *More* button for that user.

User Accounts Control Table - Add	
User Name	wadayulukinat
New Password	*****
Confirm New Password	*****
Access Right	Root
<input type="button" value="Apply"/>	

**Figure7- 42. Add User Accounts Control Table**

Add a new user by typing in a **User Name**, and **New Password** and retype the same password in the **Confirm New Password**. Choose the level of privilege (*Root, User* or *User+*) from the **Access Right** drop-down menu.

User Accounts Control Table - Edit	
User Name	tonyisagod
New Password	*****
Confirm New Password	*****
Access Right	Root
<input type="button" value="Apply"/> <input type="button" value="Delete"/>	

**Figure7- 43. Edit User Accounts Table**

Modify or delete an existing user account in the User Account Control Table – Edit. To delete the user account, click on the *Delete* button. To change the password, type in the **New Password** and retype it in the **Confirm New Password** entry field. Choose the level of privilege (*Root, User* or *User+*) from the **Access Right** drop-down menu.

## Serial Port Settings

Change serial port settings by clicking on the Serial Port Settings button to see the screen shown below. Change the Auto-logout console settings or change the SLIP settings.

Figure7- 44. Serial Port Settings

### Console Settings

The read-only console settings are:

<b>Baud Rate</b>	Specifies the rate data will be exchanged over the serial link. The default value is 9600 baud.
<b>Data Bits</b>	Specifies the number of bits that will carry data over the serial link. The default value is 8 bits.
<b>Stop Bits</b>	Specifies the number of bits that indicate when a serial word ends. The default value is 1 bit.

The Auto-logout settings can be changed. Select *2 minutes*, *5 minutes*, *10 minutes*, *15 minutes* or *Never* from the drop-down menu.

### **SLIP Settings**

Change the following SLIP settings:

<b>Baud Rate</b>	Specifies the rate data will be exchanged over the serial link. The default value is 9600 baud.
<b>Interface Name</b>	The name of the IP interface, previously defined on the switch, that will communicate with the remote management station.
<b>Local IP Address</b>	The IP address that corresponds to the IP interface name above.
<b>Remote IP Address</b>	The IP address of the remote management station that will communicate with the switch using SLIP.
<b>MTU</b>	Maximum Transfer Unit, specifies the maximum number of bytes (octets) that can be transferred in a single packet. The options are 1006 and 1500.



## Monitoring

This category includes: Port Utilization, Packets (Received (RX), UMB\_cast (RX), and Transmitted (TX)), Errors (Received (RX) and Transmitted (TX)), Size (Received (RX)), MAC Address, IGMP Snooping 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.

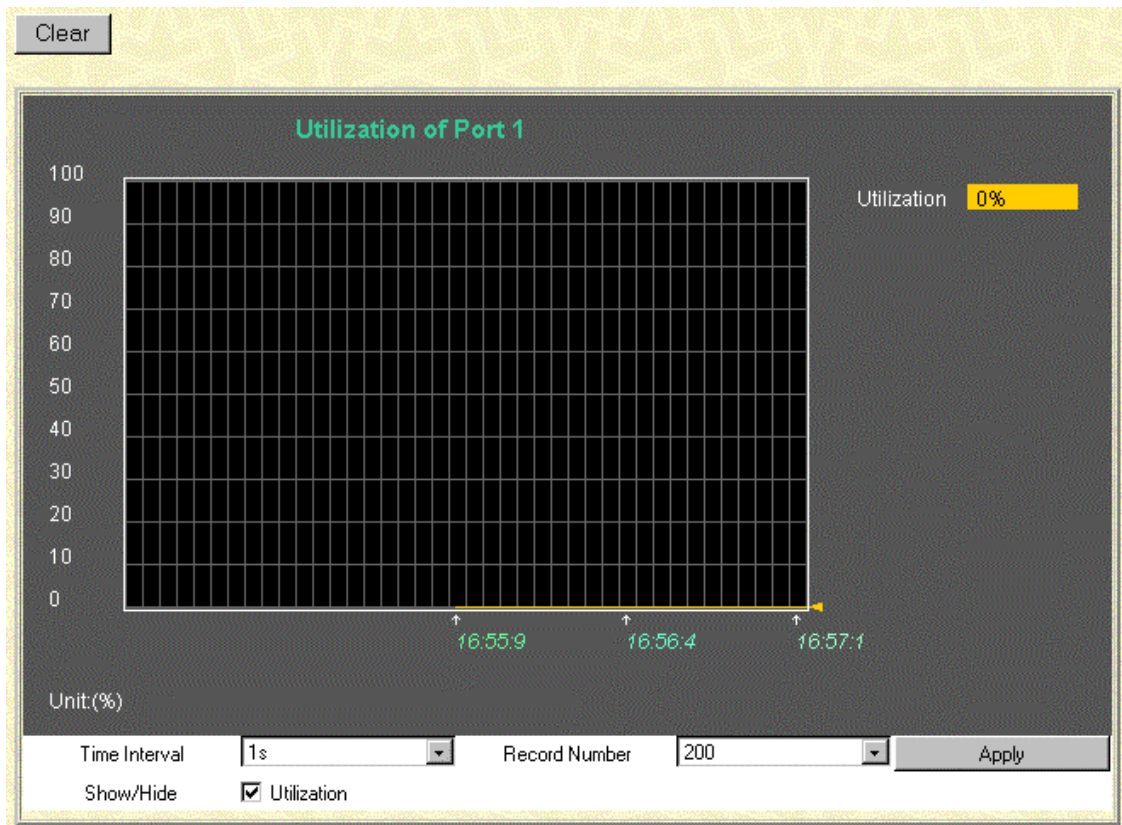


Figure7- 45. Utilization window

The information is described as follows:

<b>Time Interval</b>	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 20.
<b>Show/Hide</b>	Check whether or not to display Utilization.
<b>Clear</b>	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)

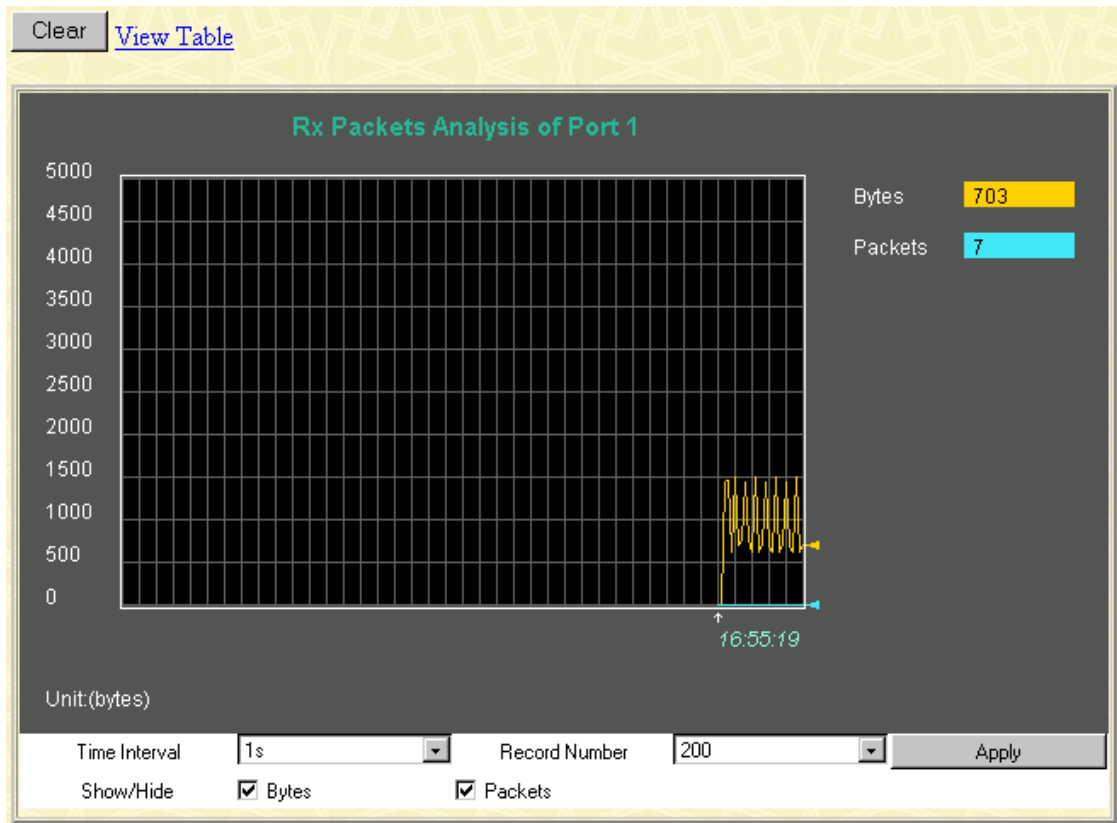


Figure7- 46. Rx Packets Analysis window (Line Chart)

[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

Figure7- 47. Rx Packets Analysis window (Table)

The information is described as follows:

<b>Time Interval</b>	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 20.
<b>Bytes</b>	Counts the number of bytes received on the port.
<b>Packets</b>	Counts the number of packets received on the port.
<b>Show/Hide</b>	Check whether or not to display Bytes and Packets.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.

### UMB-cast (RX)

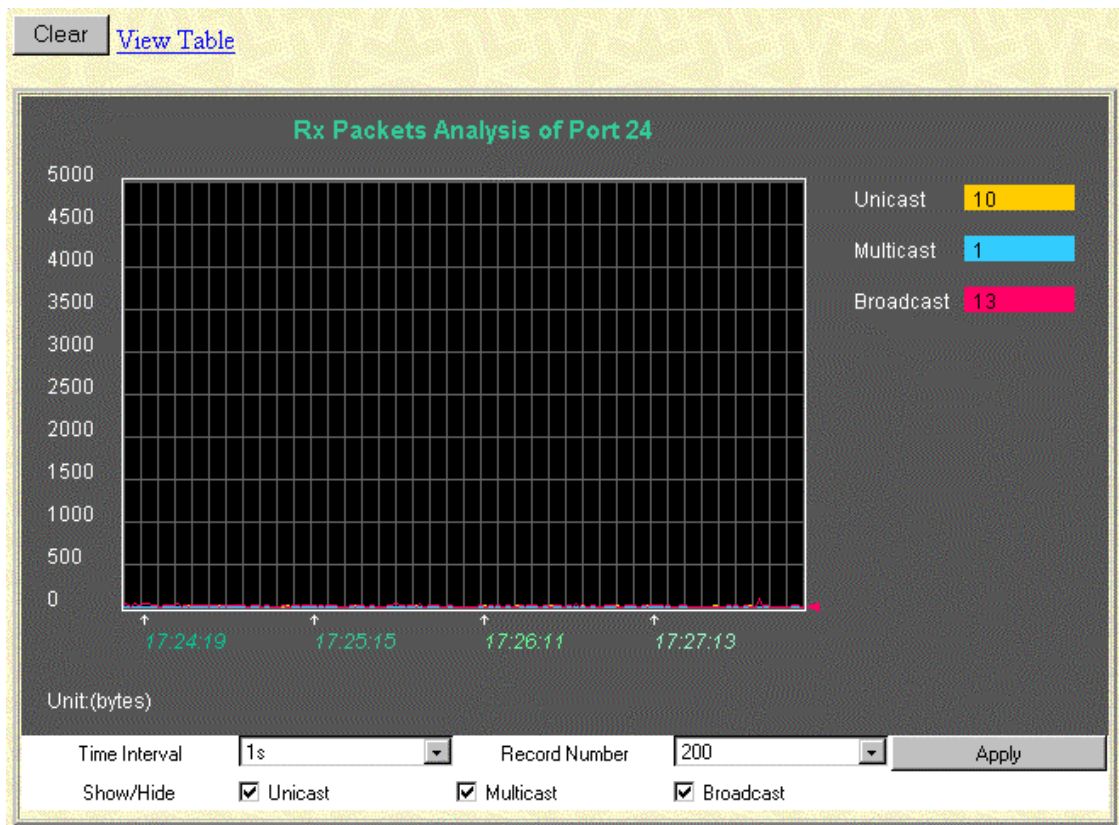
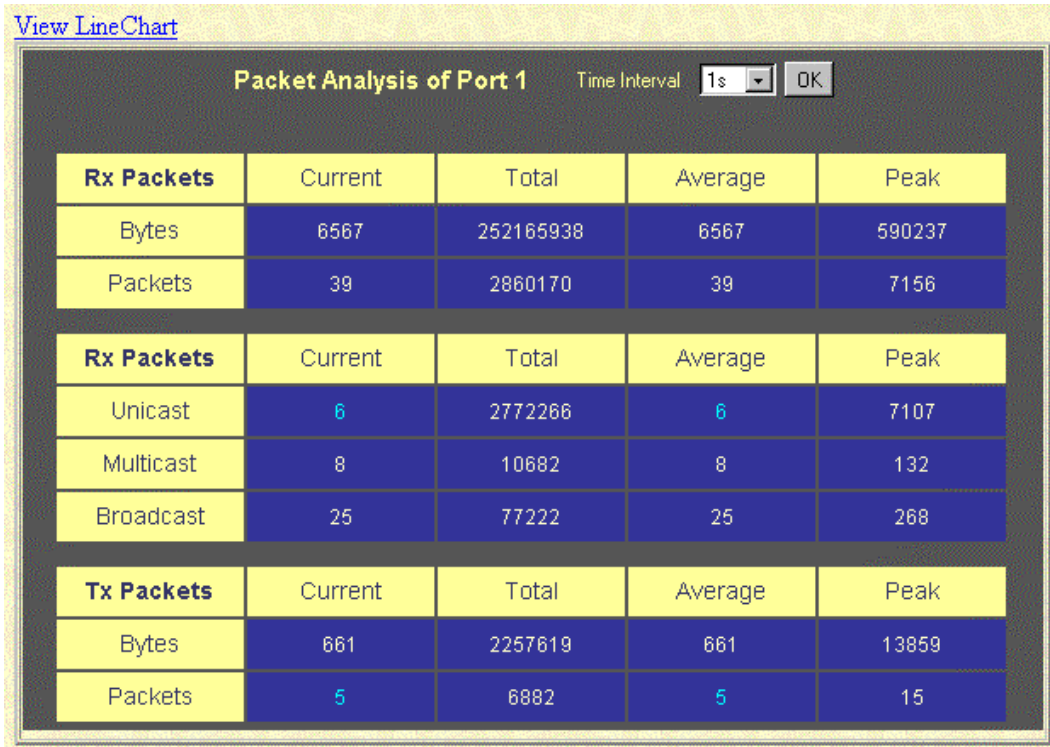


Figure7- 48. Rx Packets Analysis window for UMB (Line Chart)



**Figure7- 49. Rx Packets Analysis window for MBU (Table)**

The information is described as follows:

<b>Time Interval</b>	Select the desired setting between 1s and 60s, where “s” stands for seconds.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200.
<b>Unicast</b>	Counts the total number of good packets that were received by a unicast address.
<b>Multicast</b>	Counts the total number of good packets that were received by a multicast address.
<b>Broadcast</b>	Counts the total number of good packets that were received by a broadcast address.
<b>Show/Hide</b>	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.

### Transmitted (TX)

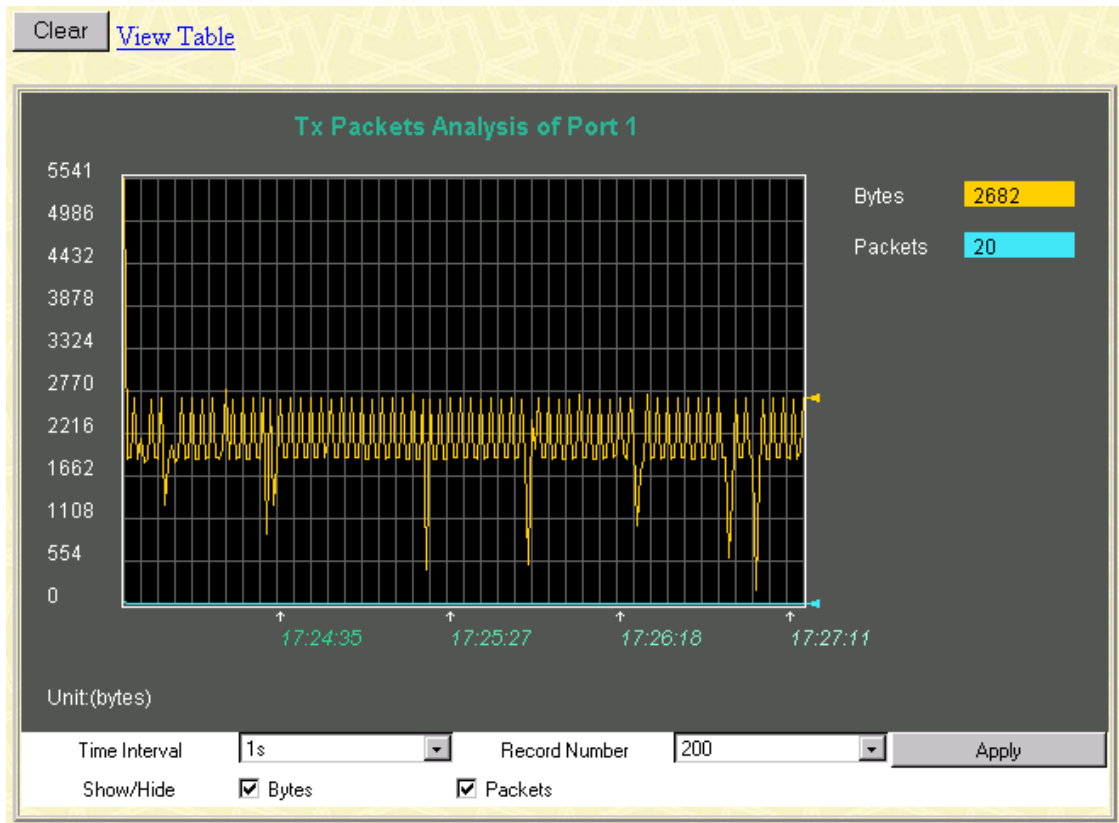


Figure7- 50. Tx Packets Analysis window (Line Chart)

[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	2772286	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

Figure7- 51. Tx Packets Analysis window (Table)

The information is described as follows:

<b>Time Interval</b>	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 20.
<b>Bytes</b>	Counts the number of bytes successfully sent from the port.
<b>Packets</b>	Counts the number of packets successfully sent on the port.
<b>Show/Hide</b>	Check whether or not to display Bytes and Packets.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	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)

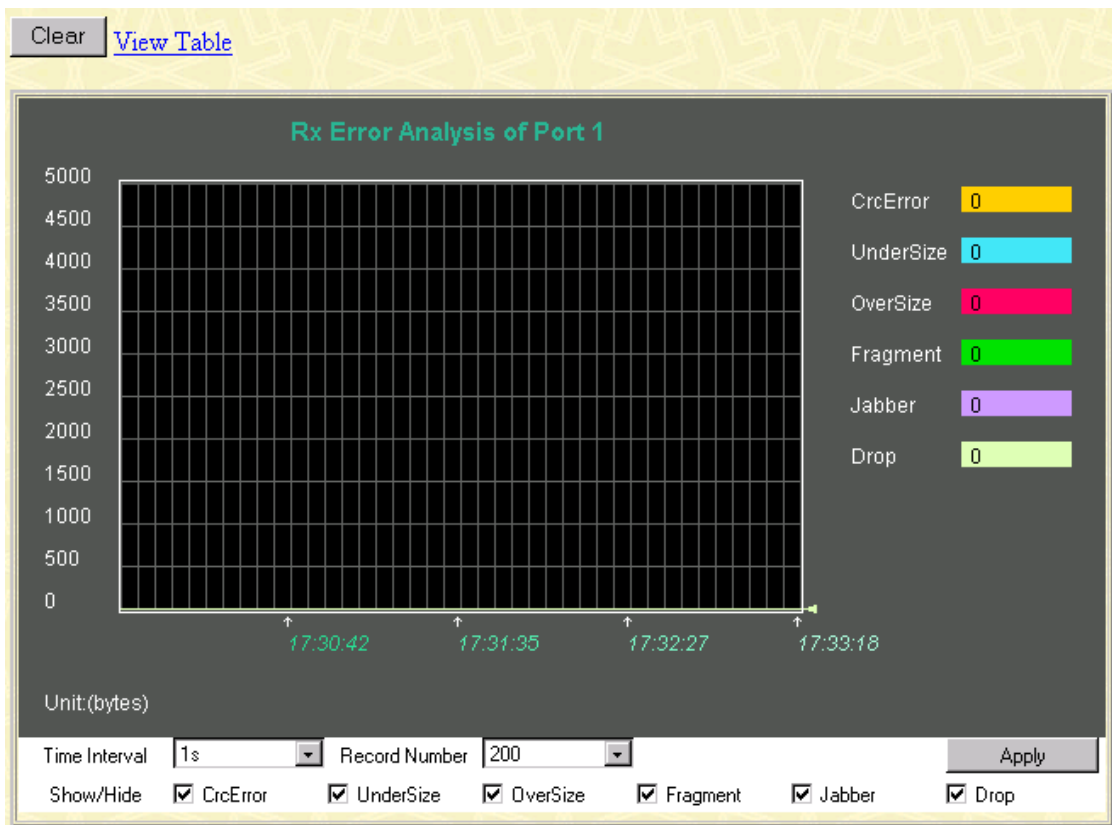
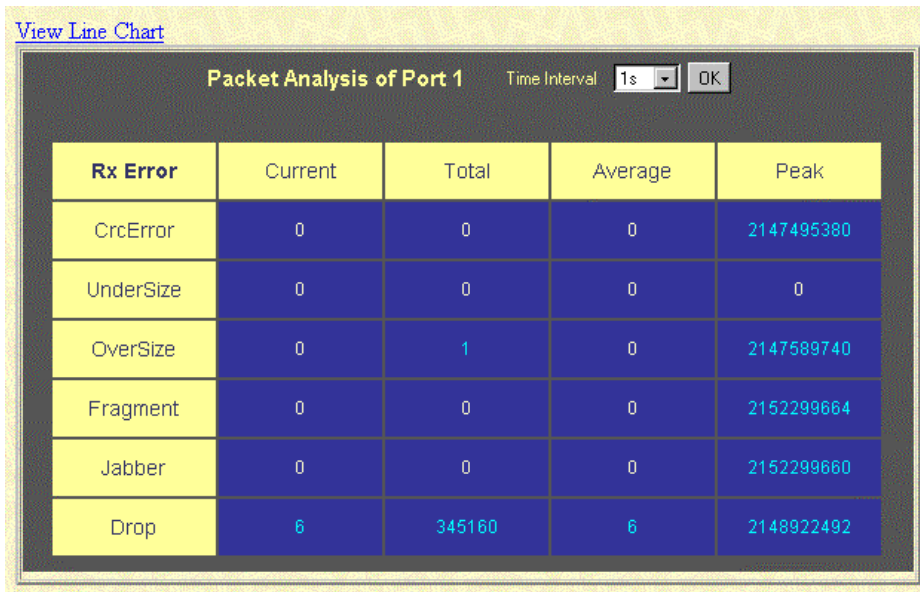


Figure7- 52. Rx Error Analysis window (Line Chart)



**Figure7- 53. Rx Error Analysis window (Table)**

The information is described as follows:

<b>Time Interval</b>	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 20.
<b>CRCErrror</b>	Counts otherwise valid frames that did not end on a byte (octet) boundary.
<b>UnderSize</b>	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.
<b>OverSize</b>	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.
<b>Fragment</b>	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
<b>Jabber</b>	The number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522
<b>Drop</b>	The number of frames which are dropped by this port since the last Switch reboot.
<b>Show/Hide</b>	Check whether or not to display CrcError, UnderSize, OverSize, Fragment, Jabber, and Drop errors.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.

## Transmitted (TX)

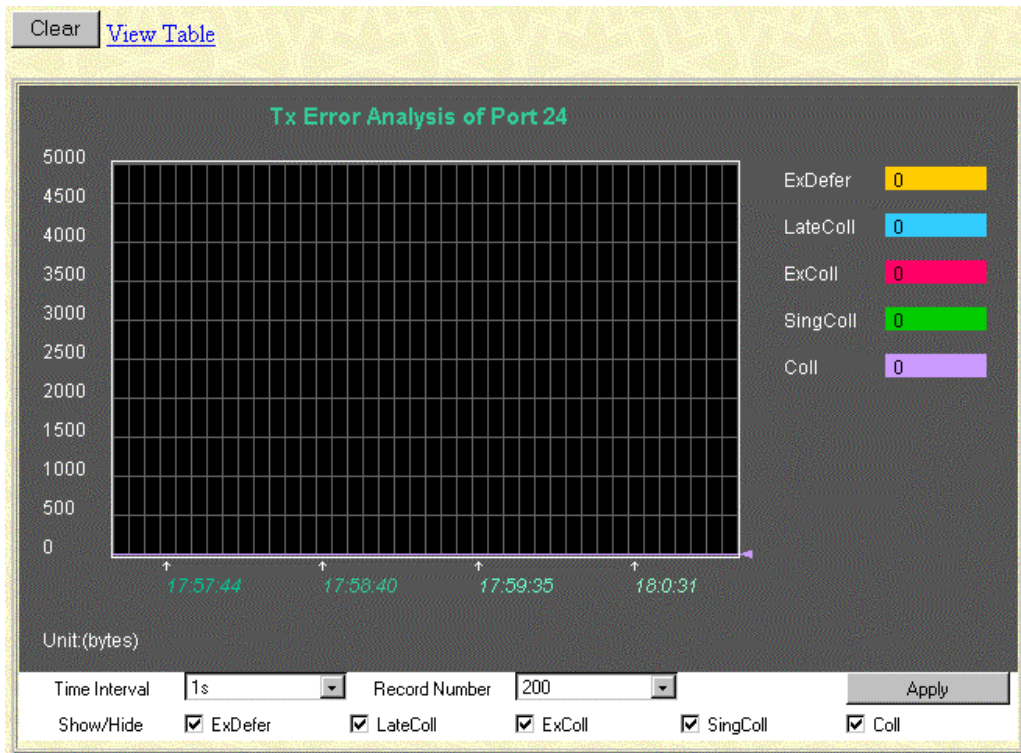


Figure7- 54. Tx Error Analysis window (Line Chart)

[View Line Chart](#)

**Packet Analysis of Port 1** Time Interval: 1s OK

Tx Error	Current	Total	Average	Peak
ExDefer	0	0	0	2152299944
CrcError	4294967295	0	0	20
LateColl	0	0	0	2152520292
ExColl	0	0	0	1
SingColl	0	0	0	1
Coll	0	0	0	1

Figure7- 55. Tx Error Analysis window (Table)



The information is described as follows:

<b>Time Interval</b>	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 20.
<b>ExDefer</b>	Counts the number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
<b>CRCErr</b>	Counts otherwise valid frames that did not end on a byte (octet) boundary.
<b>LateColl</b>	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
<b>Show/Hide</b>	Check whether or not to display ExDefer, CrcError, and LateColl errors.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	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

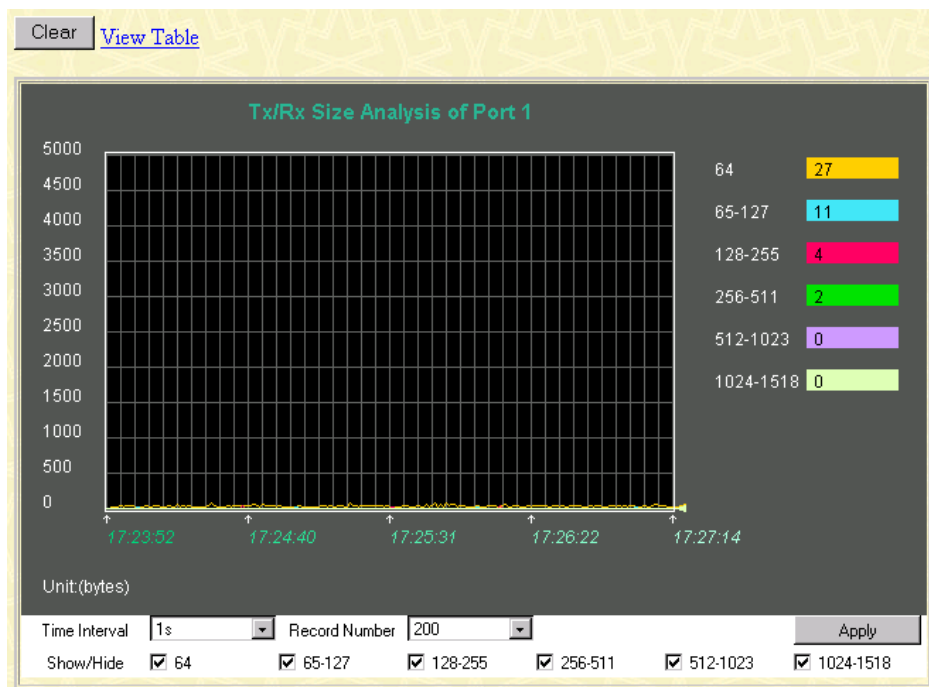


Figure7- 56. Tx/Rx Size Analysis window (Line Chart)

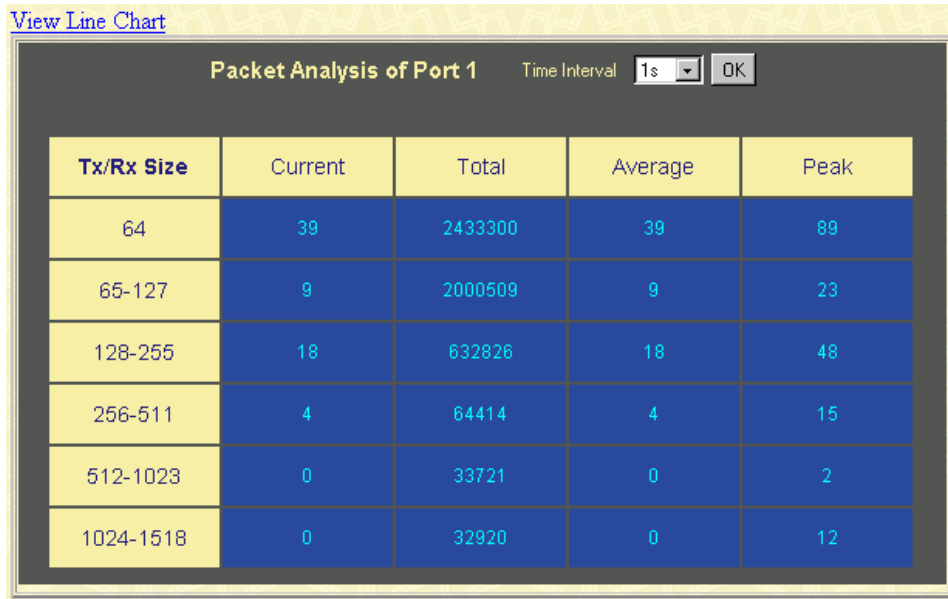


Figure7- 57. Packet Analysis window (Table)

The information is described as follows:

<b>Time Interval</b>	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 20.
<b>64</b>	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
<b>65-127</b>	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).
<b>128–255</b>	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).
<b>256-511</b>	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).
<b>512-1023</b>	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).
<b>1024-1518</b>	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).
<b>Show/Hide</b>	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	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:

The screenshot shows the 'Browse Address Table - sequential' window. At the top, there are three search options: 'Search Table By VID' (with an empty input field), 'Search Table By MAC Address' (with '00-00-00-00-00-00' entered), and 'Search Table By Port' (with 'Unit 1' and 'Port 1' selected). Below these are 'Clear Table By Port' and 'Clear All Table' buttons. The main table has the following data:

Unit	VID	MAC Address	Port	Learned
1	1	00-00-00-00-00-08	S1P1	dynamic
1	1	00-00-00-00-00-09	S1P1	dynamic
1	1	00-00-00-33-33-00	S1P1	dynamic
1	1	00-00-80-50-12-34	S1P1	dynamic
1	1	00-00-81-9a-a0-9f	S1P1	dynamic
1	1	00-00-81-9a-f2-f4	S1P1	dynamic
1	1	00-00-81-b6-59-dd	S1P1	dynamic
1	1	00-00-e2-4f-57-03	S1P1	dynamic
1	1	00-00-e2-6b-bc-f6	S1P1	dynamic
1	1	00-00-f8-7c-1c-28	S1P1	dynamic
1	1	00-00-f8-7c-1c-29	S1P1	dynamic
1	1	00-01-02-03-04-05	S1P1	dynamic
1	1	00-01-30-fa-5f-00	S1P1	dynamic
1	1	00-01-96-9c-06-00	S1P1	dynamic
1	1	00-02-3f-70-d8-fe	S1P1	dynamic
1	1	00-02-3f-71-3e-ce	S1P1	dynamic
1	1	00-02-a5-fa-bd-95	S1P1	dynamic
1	1	00-03-47-74-c8-91	S1P1	dynamic
1	1	00-03-6d-1e-76-79	S1P1	dynamic
1	1	00-03-7f-be-f1-f4	S1P1	dynamic

At the bottom, it shows 'Total Addresses in Table: 448' and a 'Next' button.

Figure7- 58. MAC Address Table window

The information is described as follows:

<b>Search by VLAN ID</b>	Allows the forwarding table to be browsed by VLAN ID (VID).
<b>Search by MAC Address</b>	Allows the forwarding table to be browsed by MAC Address.
<b>Search by Port</b>	Allows the forwarding table to be browsed by port number.
<b>Jump</b>	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
<b>Find</b>	Click the icon to find the data entry.
<b>Clear All</b>	Clears all forwarding table entries.
<b>Clear By Port</b>	Clears the forwarding table entries that have the entered port number.
<b>VID</b>	The VLAN ID of the VLAN the port is a member of.
<b>MAC Address</b>	The MAC address entered into the address table.
<b>Port</b>	The port that the MAC address above corresponds to.
<b>Learned</b>	How the switch discovered the MAC address. The possible entries are <i>Dynamic</i> , <i>Self</i> , and <i>Static</i> .
<b>Next</b>	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).

IGMP Snooping Table				
Unit	State	Age out	Querier State	View
1	Disabled	260	Non-Querier	View

Total Vlan entries in the table :0

IGMP Monitor														
Multicast Group	MAC Address	Port Map												Reports
		1	2	3	4	5	6	7	8	9	10	11	12	
		13	14	15	16	17	18	19	20	21	22	23	24	

Figure7- 59. IGMP Snooping Table window

The information is described as follows:

<b>VID</b>	VLAN ID of the VLAN for which the IGMP Snooping table is to be displayed.
<b>Search</b>	Click on the View button to display the IGMP Snooping Table for the current VID.
<b>Multicast Group</b>	The IP address of a multicast group learned by IGMP snooping.
<b>MAC Address</b>	The corresponding MAC address learned by IGMP snooping.
<b>Port Map</b>	Displays the ports that have forwarded multicast packets.
<b>Reports</b>	The number of IGMP reports for the listed source.

## Port Access Control

There are five windows that comprise the 802.1X port-based authentication section.

### Authenticator State

Authenticator Status of Unit 1								
						Time Interval	1s	OK
Port	AuthState	BackendState	AdmDir	OprDir	PortStatus	PortControl		
1	N/A	-	-	-	-	-		
2	N/A	-	-	-	-	-		
3	N/A	-	-	-	-	-		
4	N/A	-	-	-	-	-		
5	N/A	-	-	-	-	-		
6	N/A	-	-	-	-	-		

Figure7- 60. 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.

### Authenticator Statistics

Show Authenticator Statistics of Unit 1								
						Time Interval	1s	OK
Port	Tx ReqId	Tx Req	Rx Start	Rx LogOff	Rx Respld	Rx Error		
1	0	0	0	0	0	0		
2	0	0	0	0	0	0		
3	0	0	0	0	0	0		
4	0	0	0	0	0	0		
5	0	0	0	0	0	0		
6	0	0	0	0	0	0		

Figure7- 61. 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.

### Authenticator Session-Counter

Port	Frames Rx	Frames Tx	UserName	Time	TerminateCause
1	0	0		0	N/A
2	0	0		0	N/A
3	0	0		0	N/A
4	0	0		0	N/A
5	0	0		0	N/A
6	0	0		0	N/A

Figure7- 62. 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.

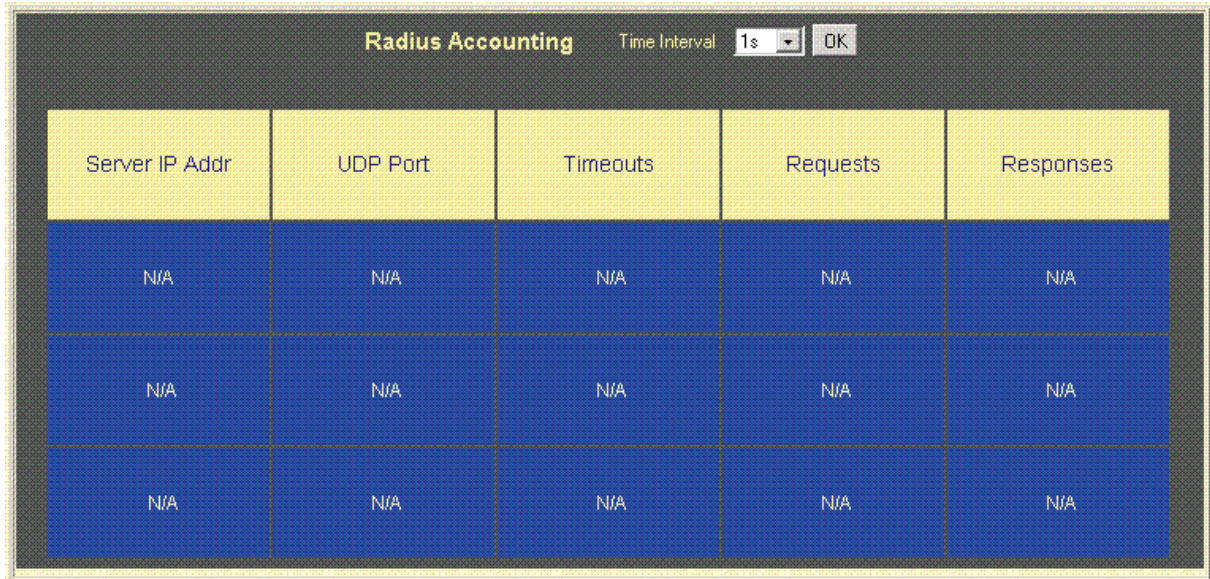
### Radius Authentication

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

Figure7- 63. Show 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.

## Radius Accounting



The screenshot shows a window titled "Radius Accounting" with a "Time Interval" dropdown menu set to "1s" and an "OK" button. Below the header is a table with five columns: "Server IP Addr", "UDP Port", "Timeouts", "Requests", and "Responses". The table contains three rows of data, all of which are "N/A".

Server IP Addr	UDP Port	Timeouts	Requests	Responses
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

**Figure7- 64. Show 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.

## Maintenance

This category includes TFTP Services (Update Firmware, Configuration File, Save Settings, and Save History Log), Switch History, Ping Test, Local Loopback, Line Loopback, Save Changes, Factory Reset, Restart System.

### 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

Figure7- 65. 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:

<b>Server IP Address</b>	The IP address of the TFTP server.
<b>File Name</b>	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.

Figure7- 66. 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 configuration 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.

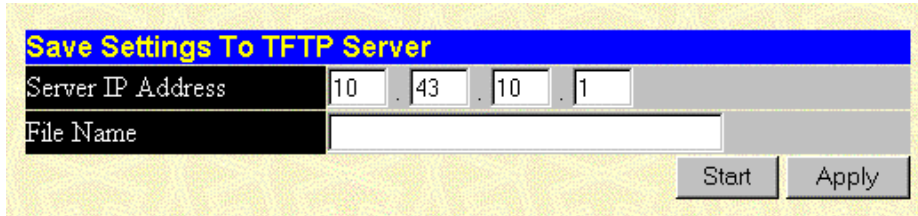
The information is described as follows:



<b>Server IP Address</b>	The IP address of the TFTP server.
<b>File Name</b>	The full file name (including path) of the new firmware file on the TFTP server.

### Save Settings

The Switch's current settings can be uploaded to a TFTP Server by the Switch's management agent.



**Figure7- 67. 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.

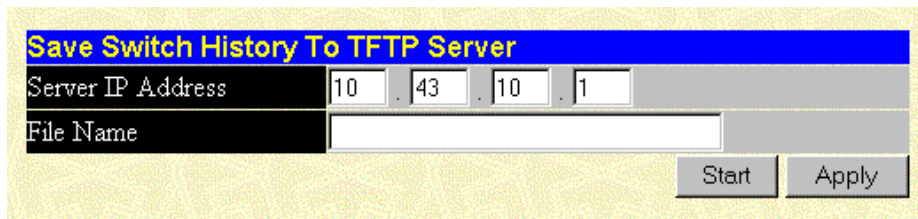
The information is described as follows:

<b>Server IP Address</b>	The IP address of the TFTP server.
<b>File Name</b>	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.



**Figure7- 68. 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.
<b>File Name</b>	The full file name (including path) of the new firmware file on the TFTP server.

## 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

Figure7- 69. 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:

<b>Sequence</b>	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
<b>Time</b>	Displays the time in days, hours, and minutes since the Switch was last restarted.
<b>Log Text</b>	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.

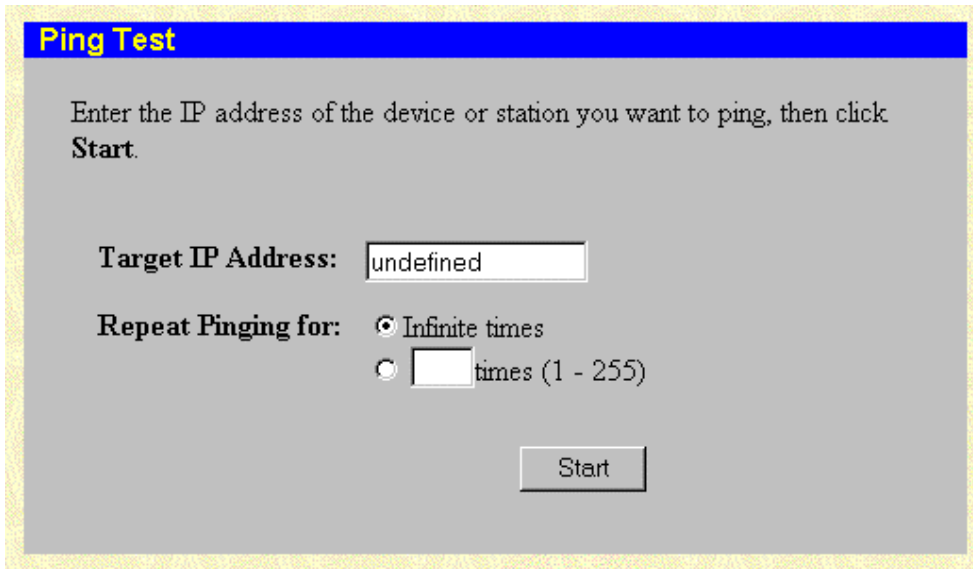


Figure7- 70. Ping Test window

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.

## Local Loopback Test

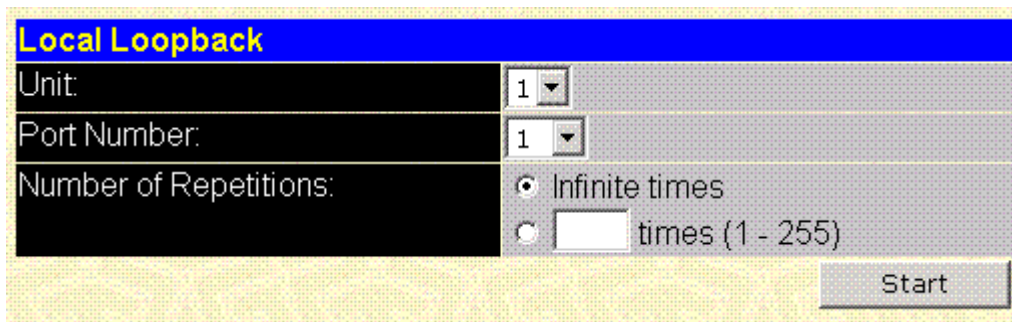
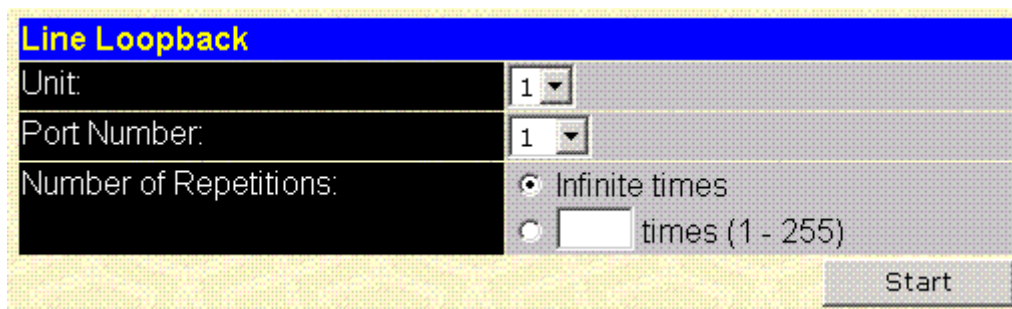


Figure7- 71. Local Loopback Test Screen

To perform a local loopback test, select the **Port Number:** of the target port and the number of repetitions. If you choose Infinite times the test can be stopped and resumed by clicking on the appropriate button.

## Line Loopback Test



### Figure7- 72. Line Loopback Test Screen

To perform a line loopback test, select the **Port Number:** of the target port and the number of repetitions. If you choose Infinite times the test can be stopped and resumed by clicking on the appropriate button.

### Save Changes

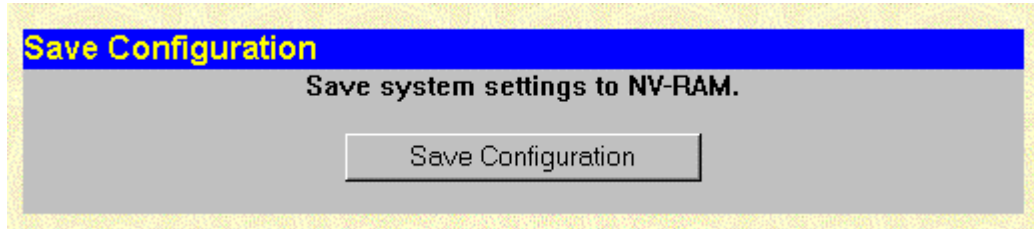


Figure7- 73. Save Configuration window

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

### Factory Reset

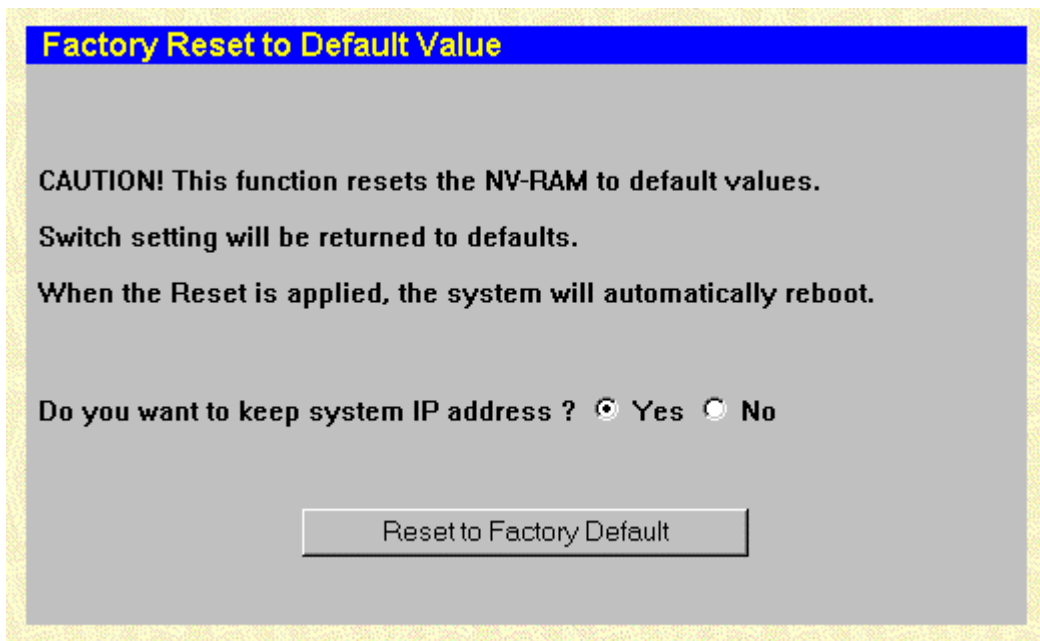


Figure7- 74. Factory Reset to Default Value window

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



**Figure7- 75. Restart System window**

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



## Technical Specifications

General	
<b>STANDARDS:</b>	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.1 Q VLAN IEEE 802.3x Full-duplex Flow Control
<b>TOPOLOGY:</b>	Star
<b>NETWORK CABLES:</b>	Telco50 (RJ-21) Cat.5 Ethernet (RJ-45) 24AWG (RJ-11) IEEE 1394 specifications can be downloaded from: <a href="http://www.1394ta.org/Technology/Specifications/specifications.htm">http://www.1394ta.org/Technology/Specifications/specifications.htm</a>

Physical and Environmental	
<b>AC inputs:</b>	100 - 240 VAC, 50/60 Hz (internal universal power supply)
<b>Power Consumption:</b>	75 watts maximum
<b>DC fans:</b>	3 built-in 40 x 40 x 10 mm fans for main board 1 built-in 40 x 40 x 10 mm for power supply
<b>Operating Temperature:</b>	0 to 40 degrees Celsius
<b>Storage Temperature:</b>	-25 to 55 degrees Celsius
<b>Humidity:</b>	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
<b>Dimensions:</b>	441 mm x 387 mm x 44 mm (1U), 19 inch rack-mount width
<b>Weight:</b>	6 kg
<b>EMI:</b>	FCC Class A, CE Class A, VCCI Class A, BSMI Class A, C-Tick Class A
<b>Safety:</b>	UL/CUL

Performance	
<b>Transmission Method:</b>	Store-and-forward
<b>RAM Buffer:</b>	8 Mbytes per device
<b>Filtering Address Table:</b>	8K
<b>MAC Address Learning:</b>	Automatic update.
<b>Forwarding Table Age Time:</b>	Max age: 10 - 1000000 seconds. Default = 300.

24 Port Splitter Low Pass Filter	
<b>Passband Frequency:</b>	DC to 125KHz
<b>Insertion Loss:</b>	0.7dB maximum @20KHz ~ 125KHz
<b>Return Loss:</b>	20dB minimum @DC to 100KHz 15dB minimum @100KHz ~ 125KHz
<b>Stopband Frequency:</b>	800KHz ~ 7.9MHz
<b>Attenuation:</b>	65dB minimum
<b>Impedance:</b>	150Ω
<b>Operating Temperature:</b>	-10 to 60 degrees Celsius



## ***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
Console time out	10 min
User name	None
Password	None
Device STP	Disable
Port STP	Enable
Port enable	Enable
Bridge max age	20 secs
Bridge hello time	2 sec
Bridge forward delay	15 sec
Bridge priority	32768
Port STP cost	100
Port STP priority	128
Forwarding table aging time	300 secs
NWay	Enable
Flow control	Enable
Community string	"public", "private"
VLAN mode	IEEE 802.1Q
SNMP VLAN(802.1Q)	1
Default port VID	1
Ingress rule checking	Disable



# D-Link® Offices

---

## Australia

### D-Link Australasia

Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069 Australia  
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE (Australia): 1800-177100  
TOLL FREE (New Zealand): 0800-900900  
URL: [www.dlink.com.au](http://www.dlink.com.au) E-MAIL: [support@dlink.com.au](mailto:support@dlink.com.au) & [info@dlink.com.au](mailto:info@dlink.com.au)

Level 1, 434 St. Kilda Road, Melbourne, Victoria 3004 Australia  
TEL: 61-3-9281-3232 FAX: 61-3-9281-3229 MOBILE: 0412-660-064

## Canada

### D-Link Canada

2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada  
TEL: 1-905-829-5033 FAX: 1-905-829-5095 BBS: 1-965-279-8732  
TOLL FREE: 1-800-354-6522 URL: [www.dlink.ca](http://www.dlink.ca)  
FTP: [ftp.dlinknet.com](ftp://ftp.dlinknet.com) E-MAIL: [techsup@dlink.ca](mailto:techsup@dlink.ca)

## Chile

### D-Link South America

Isidora Goyechea 2934 of 702, Las Condes, Santiago, Chile, S. A.  
TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: [www.dlink.cl](http://www.dlink.cl)  
E-MAIL: [ccasassu@dlink.cl](mailto:ccasassu@dlink.cl) & [tsilva@dlink.cl](mailto:tsilva@dlink.cl)

## China

### D-Link China

2F, Sigma Building, 49 Zhichun Road, Haidan District, 100080 Beijing, China  
TEL: 86-10-88097777 FAX: 86-10-88096789 URL: [www.dlink.com.cn](http://www.dlink.com.cn)  
E-MAIL: [liweii@digitalchina.com.cn](mailto:liweii@digitalchina.com.cn)

## Denmark

### D-Link Denmark

Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark  
TEL: 45-43-969040 FAX: 45-43-424347 URL: [www.dlink.dk](http://www.dlink.dk) E-MAIL: [info@dlink.dk](mailto:info@dlink.dk)

## Egypt

### D-Link Middle East

7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt  
TEL: 20-2-635-6176 FAX: 20-2-635-6192 URL: [www.dlink-me.com](http://www.dlink-me.com)  
E-MAIL: [support@dlink-me.com](mailto:support@dlink-me.com) & [fateen@dlink-me.com](mailto:fateen@dlink-me.com)

## Finland

### D-Link Finland

Thlli-ja Pakkahuone Katajanokanlaituri 5, FIN- 00160 Helsinki  
TEL: 358-9-622-91660 FAX: 358-9-622-91661 URL: [www.dlink-fi.com](http://www.dlink-fi.com)

## France

### D-Link France

Le Florilege #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](http://www.dlink-france.fr)  
E-MAIL: [info@dlink-france.fr](mailto: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](http://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](mailto:info@dlink.de)

## India

### D-Link India

Plot No.5, Kurla-Bandra Complex Rd., Off Cst Rd., Santacruz (E), Bombay, 400 098 India  
TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: [www.dlink-india.com](http://www.dlink-india.com)  
E-MAIL: [service@dlink.india.com](mailto:service@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](http://www.dlink.it) E-MAIL: [info@dlink.it](mailto:info@dlink.it)

<b>Japan</b>	<b>D-Link Japan</b> 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
<b>Netherlands</b>	<b>D-Link Benelux</b> Fellenoord 1305611 ZB, Eindhoven, the Netherlands TEL: 31-40-2668713 FAX: 31-40-2668666 URL: www.d-link-benelux.nl
<b>Norway</b>	<b>D-Link Norway</b> Waldemar Thranesgt. 77, 0175 Oslo, Norway TEL: 47-22-991890 FAX: 47-22-207039
<b>Russia</b>	<b>D-Link Russia</b> 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
<b>Singapore</b>	<b>D-Link International</b> 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com
<b>South Africa</b>	<b>D-Link South Africa</b> 102 – 106 Witchazel Avenue, Einstein Park 2, Block B, Highveld Technopark, Centurion, South Africa TEL: 27 (0) 12-665-2165 FAX: 27 (0) 12-665-2186 URL: www.d-link.co.za E-MAIL: attie@d-link.co.za
<b>Spain</b>	<b>D-Link Iberia</b> C/Sabino De Arana, 56 Bajos, 08028 Barcelona, Spain TEL: 34 93 4090770 FAX: 34 93 4910795 URL: www.dlinkiberia.es E-MAIL: info@dlinkiberia.es
<b>Sweden</b>	<b>D-Link Sweden</b> P. O. Box 15036, S-167 15 Bromma, Sweden TEL: 46-(0) 8-564-61900 FAX: 46-(0) 8-564-61901 E-MAIL: info@dlink.se URL: www.dlink.se
<b>Taiwan</b>	<b>D-Link Taiwan</b> 2F, No. 119 Pao-Chung Rd, 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
<b>Turkey</b>	<b>D-Link Middle East</b> 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
<b>U.A.E.</b>	<b>D-Link Middle East</b> CHS Aptec (Dubai), P.O. Box 33550 Dubai U.A.E. TEL: 971-4-366-885 FAX: 971-4-355-941 E-MAIL: Wxavier@dlink-me.com
<b>U.K.</b>	<b>D-Link Europe</b> 4 <sup>th</sup> Floor, Merit House, Edgware Road, Colindale, London NW9 5AB United Kingdom TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 BBS: 44 (0) 181-235-5511 URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk
<b>U.S.A.</b>	<b>D-Link U.S.A.</b> 53 Discovery Drive, Irvine, CA 92618, USA TEL: 1-949-788-0805 FAX: 1-949-753-7033 BBS: 1-949-455-1779 & 1-949-455-9616 INFO: 1-800-326-1688 URL: www.dlink.com E-MAIL: tech@dlink.com & support@dlink.com

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>