



# VES1724-56

24-port Temperature-Hardened VDSL2 Box DSLAM

Version 3.80  
Edition 1, 9/2013

## User's Guide

### Default Login Details

LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

---

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

### **Related Documentation**

- Support Disc

Refer to the included CD for support documents.

# Contents Overview

<b>User's Guide .....</b>	<b>17</b>
Getting to Know Your Switch .....	19
Hardware Installation and Connection .....	23
Hardware Overview .....	26
The Web Configurator .....	33
Initial Setup Example .....	42
Tutorials .....	46
<b>Technical Reference .....</b>	<b>51</b>
System Status and Port Statistics .....	53
Basic Setting .....	70
VDSL Setup .....	97
VLAN .....	129
Static MAC Forward Setup .....	152
Static Multicast Forward Setup .....	154
Filtering .....	158
Spanning Tree Protocol .....	160
Broadcast Storm Control .....	176
Mirroring .....	178
Link Aggregation .....	180
Port Authentication .....	186
MAC Limit .....	191
Classifier .....	194
Policy Rule .....	200
Queuing Method .....	205
VLAN Stacking .....	208
Multicast .....	217
Authentication and Accounting .....	236
IP Source Guard .....	249
Loop Guard .....	270
CFM .....	274
VLAN Mapping .....	278
Layer 2 Protocol Tunneling .....	282
DoS Prevention .....	286
PPPoE IA .....	288
Static Route .....	301
Differentiated Services .....	304
DHCP .....	311

Maintenance .....327  
Access Control ..... 334  
Diagnostic ..... 356  
Syslog ..... 358  
Loop Diagnostic ..... 361  
MAC Table ..... 365  
ARP Table ..... 367  
Hardware Information ..... 369  
CFM Action ..... 370  
IPv6 Cache ..... 372  
Troubleshooting ..... 377  
Product Specifications ..... 381

# Table of Contents

<b>Contents Overview .....</b>	<b>3</b>
<b>Table of Contents .....</b>	<b>5</b>
<b>Part I: User's Guide .....</b>	<b>17</b>
<b>Chapter 1</b>	
<b>Getting to Know Your Switch.....</b>	<b>19</b>
1.1 Introduction .....	19
1.2 Applications .....	19
1.2.1 MTU Application .....	19
1.2.2 Curbside Application .....	20
1.3 Ways to Manage the Switch .....	21
1.4 Good Habits for Managing the Switch .....	21
<b>Chapter 2</b>	
<b>Hardware Installation and Connection .....</b>	<b>23</b>
2.1 Installation Scenarios .....	23
2.2 Desktop Installation Procedure .....	23
2.3 Mounting the Switch on a Rack .....	24
2.3.1 Rack-mounted Installation Requirements .....	24
2.3.2 Attaching the Mounting Brackets to the Switch .....	24
2.3.3 Mounting the Switch on a Rack .....	25
2.4 Connecting the Frame Ground .....	25
<b>Chapter 3</b>	
<b>Hardware Overview .....</b>	<b>26</b>
3.1 Front Panel .....	26
3.1.1 Power Connector .....	26
3.1.2 Gigabit Ethernet Ports .....	27
3.1.3 Mini-GBIC Slots .....	28
3.1.4 Management Port .....	29
3.1.5 Console Port .....	30
3.1.6 ALARM Slot .....	30
3.2 LEDs .....	31
<b>Chapter 4</b>	
<b>The Web Configurator .....</b>	<b>33</b>

4.1 Introduction .....	33
4.2 System Login .....	33
4.3 The Port Status Screen .....	34
4.3.1 Change Your Password .....	39
4.4 Saving Your Configuration .....	39
4.5 Switch Lockout .....	39
4.6 Resetting the Switch .....	40
4.6.1 Reload the Configuration File .....	40
4.7 Logging Out of the Web Configurator .....	41
4.8 Help .....	41
<b>Chapter 5</b>	
<b>Initial Setup Example.....</b>	<b>42</b>
5.1 Overview .....	42
5.2 Configuring Switch Management IP Address .....	42
5.2.1 Creating a VLAN .....	43
5.2.2 Setting Port VID .....	44
<b>Chapter 6</b>	
<b>Tutorials.....</b>	<b>46</b>
6.1 How to Use DHCP Relay Per VLAN on the Switch .....	46
6.1.1 DHCP Relay Tutorial Introduction .....	46
6.1.2 Creating a VLAN .....	46
6.1.3 Configuring Management IP Address .....	48
6.1.4 Configuring DHCP VLAN Settings .....	49
6.1.5 Testing the Connection .....	50
<b>Part II: Technical Reference.....</b>	<b>51</b>
<b>Chapter 7</b>	
<b>System Status and Port Statistics.....</b>	<b>53</b>
7.1 Overview .....	53
7.2 Port Status Summary .....	53
7.2.1 VDSL Port Status Change .....	54
7.2.2 VDSL Port Details .....	55
7.2.3 Bonding Group Details .....	65
7.2.4 VDSL Summary .....	66
7.2.5 Port Details .....	67
<b>Chapter 8</b>	
<b>Basic Setting .....</b>	<b>70</b>

8.1 Overview .....	70
8.2 System Information .....	70
8.3 General Setup .....	72
8.4 Introduction to VLANs .....	74
8.5 Switch Setup Screen .....	75
8.6 IPv6 Introduction .....	76
8.6.1 IPv6 Addressing .....	76
8.6.2 IPv6 Prefix and Prefix Length .....	77
8.6.3 IPv6 Subnet Masking .....	77
8.6.4 Interface ID .....	77
8.6.5 Link-local Address .....	77
8.6.6 Global Address .....	77
8.6.7 Unspecified .....	78
8.6.8 EUI-64 .....	78
8.6.9 Stateless Autoconfiguration .....	78
8.7 IP Setup .....	79
8.7.1 Management IP Addresses .....	79
8.8 External Alarm Switch .....	81
8.9 Port Setup .....	82
8.10 Rate Limit Profile Setup .....	84
8.10.1 Per Queue Ratelimit Profile .....	85
8.11 Hardware Alarm Profile .....	87
8.12 CPE Port Status .....	87
8.13 IPv6 Setup .....	88
8.13.1 IPv6 Setup: Configuration .....	90
8.13.2 IPv6 ND Setup .....	91
8.13.3 IPv6 Neighbor Setup .....	91
8.14 SFP Threshold Setup .....	93
<b>Chapter 9</b>	
<b>VDSL Setup .....</b>	<b>97</b>
9.1 VDSL Overview .....	97
9.1.1 VDSL Profile Example .....	101
9.1.2 Primary and Fallback VDSL Templates Example .....	102
9.2 VDSL Line Setup .....	103
9.3 VDSL Template Setup .....	104
9.3.1 VDSL Line Profile Setup .....	106
9.3.2 VDSL Line Profile Setup > Rate Adaptive .....	109
9.3.3 VDSL Line Profile Setup > MIB PSD Mask .....	111
9.3.4 VDSL Line Profile Setup > DPBO .....	112
9.3.5 VDSL Line Profile Setup > RFI Band .....	113
9.3.6 VDSL Line Profile Setup > Virtual Noise .....	115
9.3.7 VDSL Channel Profile Setup .....	116

9.3.8 VDSL G.INP Setup .....	118
9.3.9 VDSL INM Profile Setup .....	119
9.4 VDSL Alarm Template Setup .....	121
9.4.1 VDSL Line Alarm Profile Setup .....	122
9.4.2 VDSL Channel Alarm Profile Setup .....	124
9.5 VDSL Bonding Setup .....	125
<b>Chapter 10</b>	
<b>VLAN .....</b>	<b>129</b>
10.1 Introduction to IEEE 802.1Q Tagged VLANs .....	129
10.1.1 Forwarding Tagged and Untagged Frames .....	129
10.1.2 VLAN Tagging Priority .....	130
10.2 Automatic VLAN Registration .....	130
10.2.1 GARP .....	130
10.2.2 GVRP .....	130
10.3 Port VLAN Trunking .....	131
10.4 Select the VLAN Type .....	131
10.5 Static VLAN .....	132
10.5.1 Static VLAN Status .....	132
10.5.2 VLAN Details .....	133
10.5.3 Configure a Static VLAN .....	134
10.5.4 Configure a VLAN Profile .....	135
10.5.5 Configure VLAN Port Settings .....	137
10.6 Subnet Based VLANs .....	138
10.7 Configuring Subnet Based VLAN .....	139
10.8 Protocol Based VLANs .....	141
10.9 Configuring Protocol Based VLAN .....	142
10.10 Create an IP-based VLAN Example .....	143
10.11 Configuring MAC Based VLAN .....	144
10.12 Port Based VLAN Setup .....	146
10.12.1 Configure a Port Based VLAN .....	147
10.13 VLAN Counter .....	150
<b>Chapter 11</b>	
<b>Static MAC Forward Setup.....</b>	<b>152</b>
11.1 Overview .....	152
11.2 Configuring Static MAC Forwarding .....	152
<b>Chapter 12</b>	
<b>Static Multicast Forward Setup .....</b>	<b>154</b>
12.1 Static Multicast Forwarding Overview .....	154
12.2 Configuring Static Multicast Forwarding .....	155



<b>Chapter 13</b>	
<b>Filtering.....</b>	<b>158</b>
13.1 Configure a Filtering Rule .....	158
<b>Chapter 14</b>	
<b>Spanning Tree Protocol.....</b>	<b>160</b>
14.1 STP/RSTP Overview .....	160
14.1.1 STP Terminology .....	160
14.1.2 How STP Works .....	161
14.1.3 STP Port States .....	161
14.1.4 Multiple RSTP .....	162
14.1.5 Multiple STP .....	162
14.2 Spanning Tree Protocol Status Screen .....	165
14.3 Spanning Tree Configuration .....	165
14.4 Configure Rapid Spanning Tree Protocol .....	166
14.5 Rapid Spanning Tree Protocol Status .....	167
14.6 Configure Multiple Rapid Spanning Tree Protocol .....	168
14.7 Multiple Rapid Spanning Tree Protocol Status .....	170
14.8 Configure Multiple Spanning Tree Protocol .....	171
14.9 Multiple Spanning Tree Protocol Status .....	173
<b>Chapter 15</b>	
<b>Broadcast Storm Control.....</b>	<b>176</b>
15.1 Broadcast Storm Control Setup .....	176
<b>Chapter 16</b>	
<b>Mirroring.....</b>	<b>178</b>
16.1 Port Mirroring Setup .....	178
<b>Chapter 17</b>	
<b>Link Aggregation .....</b>	<b>180</b>
17.1 Link Aggregation Overview .....	180
17.2 Dynamic Link Aggregation .....	180
17.2.1 Link Aggregation ID .....	181
17.3 Link Aggregation Status .....	181
17.4 Link Aggregation Setting .....	182
17.5 Link Aggregation Control Protocol .....	183
17.6 Static Trunking Example .....	184
<b>Chapter 18</b>	
<b>Port Authentication .....</b>	<b>186</b>
18.1 Port Authentication Overview .....	186
18.1.1 IEEE 802.1x Authentication .....	186

18.1.2 MAC Authentication .....	187
18.2 Port Authentication Configuration .....	188
18.2.1 Activate IEEE 802.1x Security .....	188
18.2.2 Activate MAC Authentication .....	189
<b>Chapter 19</b>	
<b>MAC Limit .....</b>	<b>191</b>
19.1 MAC Limit Overview .....	191
19.2 MAC Limit .....	191
19.2.1 MAC Limit: VLAN Security .....	192
<b>Chapter 20</b>	
<b>Classifier .....</b>	<b>194</b>
20.1 About the Classifier and QoS .....	194
20.2 Configuring the Classifier .....	194
20.3 Viewing and Editing Classifier Configuration .....	197
20.4 Classifier Example .....	199
<b>Chapter 21</b>	
<b>Policy Rule .....</b>	<b>200</b>
21.1 Policy Rules Overview .....	200
21.1.1 DiffServ .....	200
21.1.2 DSCP and Per-Hop Behavior .....	200
21.2 Configuring Policy Rules .....	200
21.3 Policy Example .....	204
<b>Chapter 22</b>	
<b>Queuing Method .....</b>	<b>205</b>
22.1 Queuing Method Overview .....	205
22.1.1 Strictly Priority Queuing .....	205
22.1.2 Weighted Fair Queuing .....	205
22.1.3 Weighted Round Robin Scheduling (WRR) .....	205
22.2 Configuring Queuing .....	206
<b>Chapter 23</b>	
<b>VLAN Stacking .....</b>	<b>208</b>
23.1 VLAN Stacking Overview .....	208
23.1.1 VLAN Stacking Example .....	208
23.2 VLAN Stacking Port Roles .....	209
23.3 VLAN Tag Format .....	210
23.3.1 Frame Format .....	210
23.4 Configuring VLAN Stacking .....	211
23.4.1 Port-based Q-in-Q .....	212

23.4.2 Selective Q-in-Q .....	214
23.4.3 Port-based InnerQ .....	215
<b>Chapter 24</b>	
<b>Multicast .....</b>	<b>217</b>
24.1 Multicast Overview .....	217
24.1.1 IP Multicast Addresses .....	217
24.1.2 IGMP Filtering .....	217
24.1.3 IGMP Snooping .....	217
24.1.4 IGMP Snooping and VLANs .....	218
24.1.5 IGMP Proxy .....	218
24.1.6 Multicast Listener Discovery .....	218
24.1.7 MLD Messages .....	218
24.2 Multicast Status .....	219
24.3 Multicast Setting .....	224
24.4 IGMP Snooping VLAN .....	226
24.5 IGMP Filtering Profile .....	227
24.6 MVR Overview .....	229
24.6.1 Types of MVR Ports .....	229
24.6.2 MVR Modes .....	229
24.6.3 How MVR Works .....	229
24.7 General MVR Configuration .....	230
24.8 MVR Group Configuration .....	232
24.8.1 MVR Configuration Example .....	234
<b>Chapter 25</b>	
<b>Authentication and Accounting .....</b>	<b>236</b>
25.1 Authentication, Authorization and Accounting .....	236
25.1.1 Local User Accounts .....	236
25.1.2 RADIUS and TACACS+ .....	237
25.2 Authentication and Accounting Screens .....	237
25.2.1 RADIUS Server Setup .....	237
25.2.2 TACACS+ Server Setup .....	240
25.2.3 Authentication and Accounting Setup .....	242
25.2.4 Vendor Specific Attribute .....	244
25.3 Supported RADIUS Attributes .....	245
25.3.1 Attributes Used for Authentication .....	245
25.3.2 Attributes Used for Accounting .....	246
<b>Chapter 26</b>	
<b>IP Source Guard.....</b>	<b>249</b>
26.1 IP Source Guard Overview .....	249
26.1.1 DHCP Snooping Overview .....	249

26.1.2 ARP Inspection Overview .....	251
26.2 IP Source Guard .....	253
26.3 IP Source Guard Static Binding .....	253
26.4 DHCP Snooping .....	255
26.5 DHCP Snooping Configure .....	257
26.5.1 DHCP Snooping Port Configure .....	259
26.5.2 DHCP Snooping VLAN Configure .....	260
26.6 ARP Inspection Status .....	261
26.6.1 ARP Inspection VLAN Status .....	263
26.6.2 ARP Inspection Log Status .....	264
26.7 ARP Inspection Configure .....	265
26.7.1 ARP Inspection Port Configure .....	266
26.7.2 ARP Inspection VLAN Configure .....	268
<b>Chapter 27</b>	
<b>Loop Guard .....</b>	<b>270</b>
27.1 Loop Guard Overview .....	270
27.2 Loop Guard Setup .....	272
<b>Chapter 28</b>	
<b>CFM .....</b>	<b>274</b>
28.1 CFM Overview .....	274
28.1.1 How CFM Works .....	274
28.2 CFM MA .....	275
28.3 CFM MD .....	277
<b>Chapter 29</b>	
<b>VLAN Mapping .....</b>	<b>278</b>
29.1 VLAN Mapping Overview .....	278
29.1.1 VLAN Mapping Example .....	278
29.2 Enabling VLAN Mapping .....	279
29.3 Configuring VLAN Mapping .....	280
<b>Chapter 30</b>	
<b>Layer 2 Protocol Tunneling.....</b>	<b>282</b>
30.1 Layer 2 Protocol Tunneling Overview .....	282
30.1.1 Layer 2 Protocol Tunneling Mode .....	283
30.2 Configuring Layer 2 Protocol Tunneling .....	284
<b>Chapter 31</b>	
<b>DoS Prevention .....</b>	<b>286</b>
31.1 DoS Prevention Overview .....	286
31.2 Configuring DoS Prevention .....	286

<b>Chapter 32</b>	
<b>PPPoE IA</b> .....	<b>288</b>
32.1 PPPoE Intermediate Agent Overview .....	288
32.1.1 PPPoE Intermediate Agent Tag Format .....	288
32.1.2 Sub-Option Format .....	289
32.1.3 PPPoE IA Configuration Options .....	289
32.2 The PPPoE IA Status Screen .....	290
32.3 PPPoE IA Port Tel Configuration .....	290
32.4 PPPoE IA Global Configuration .....	291
32.5 PPPoE IA VLAN Configuration .....	293
32.6 ADSL Fallback .....	295
32.6.1 PVC Configuration .....	295
32.6.2 IPPVC Configuration .....	297
32.6.3 PAEPVC Configuration .....	299
<b>Chapter 33</b>	
<b>Static Route</b> .....	<b>301</b>
33.1 Static Routing Overview .....	301
33.2 Configuring Static Routing .....	302
<b>Chapter 34</b>	
<b>Differentiated Services</b> .....	<b>304</b>
34.1 DiffServ Overview .....	304
34.1.1 DSCP and Per-Hop Behavior .....	304
34.1.2 DiffServ Network Example .....	304
34.2 Two Rate Three Color Marker Traffic Policing .....	305
34.2.1 TRTCM-Color-blind Mode .....	306
34.2.2 TRTCM-Color-aware Mode .....	306
34.3 Activating DiffServ .....	306
34.3.1 Configuring 2-Rate 3 Color Marker Settings .....	307
34.4 DSCP-to-IEEE 802.1p Priority Settings .....	309
34.4.1 Configuring DSCP Settings .....	309
<b>Chapter 35</b>	
<b>DHCP</b> .....	<b>311</b>
35.1 DHCP Overview .....	311
35.1.1 DHCP Modes .....	311
35.1.2 DHCP Configuration Options .....	311
35.2 DHCP Status .....	311
35.3 DHCP Port Tel .....	312
35.4 DHCP Relay .....	313
35.4.1 DHCP Relay Agent Information .....	313
35.4.2 DHCP Relay Agent Information Format .....	313

35.4.3 Sub-Option Format .....	313
35.4.4 Configuring DHCP Global Relay .....	314
35.4.5 Global DHCP Relay Configuration Example .....	317
35.5 Configuring DHCP VLAN Settings .....	318
35.5.1 Example: DHCP Relay for Two VLANs .....	320
35.6 DHCPv6 LDRA .....	321
35.6.1 DHCPv6 Counter .....	324
35.6.2 Snooping Configure .....	324
<b>Chapter 36</b>	
<b>Maintenance .....</b>	<b>327</b>
36.1 The Maintenance Screen .....	327
36.2 Firmware Upgrade .....	328
36.2.1 Dual Firmware Image .....	328
36.3 Restore a Configuration File .....	329
36.4 Backup a Configuration File .....	330
36.5 Load Factory Default .....	330
36.6 Save Configuration .....	331
36.7 Reboot System .....	331
36.8 FTP Command Line .....	331
36.8.1 Filename Conventions .....	331
36.8.2 FTP Command Line Procedure .....	332
36.8.3 GUI-based FTP Clients .....	333
36.8.4 FTP Restrictions .....	333
<b>Chapter 37</b>	
<b>Access Control .....</b>	<b>334</b>
37.1 Access Control Overview .....	334
37.2 The Access Control Main Screen .....	334
37.3 About SNMP .....	334
37.3.1 SNMP v3 and Security .....	335
37.3.2 Supported MIBs .....	336
37.3.3 SNMP Traps .....	336
37.3.4 Configuring SNMP .....	342
37.3.5 Configuring SNMP Trap Group .....	344
37.3.6 Setting Up Login Accounts .....	344
37.4 SSH Overview .....	346
37.5 How SSH works .....	346
37.6 SSH Implementation on the Switch .....	347
37.6.1 Requirements for Using SSH .....	347
37.7 Introduction to HTTPS .....	347
37.8 HTTPS Example .....	348
37.8.1 Internet Explorer Warning Messages .....	348

37.8.2 Mozilla Firefox Warning Messages .....	351
37.8.3 The Main Screen .....	352
37.9 Service Port Access Control .....	353
37.10 Remote Management .....	354
<b>Chapter 38</b>	
<b>Diagnostic .....</b>	<b>356</b>
38.1 Diagnostic .....	356
<b>Chapter 39</b>	
<b>Syslog .....</b>	<b>358</b>
39.1 Syslog Overview .....	358
39.2 Syslog Setup .....	359
39.3 Syslog Server Setup .....	360
<b>Chapter 40</b>	
<b>Loop Diagnostic.....</b>	<b>361</b>
40.1 Dual-End Loop Test .....	361
40.2 Single-End Loop Test (SELT) .....	363
<b>Chapter 41</b>	
<b>MAC Table .....</b>	<b>365</b>
41.1 MAC Table Overview .....	365
41.2 Viewing the MAC Table .....	366
<b>Chapter 42</b>	
<b>ARP Table .....</b>	<b>367</b>
42.1 ARP Table Overview .....	367
42.1.1 How ARP Works .....	367
42.2 Viewing the ARP Table .....	367
<b>Chapter 43</b>	
<b>Hardware Information.....</b>	<b>369</b>
43.1 Hardware Information .....	369
<b>Chapter 44</b>	
<b>CFM Action.....</b>	<b>370</b>
44.1 CFM Action .....	370
<b>Chapter 45</b>	
<b>IPv6 Cache.....</b>	<b>372</b>
45.1 Overview .....	372
45.2 Neighbor Cache .....	373

45.3 Router .....	374
45.4 Path MTU .....	375
<b>Chapter 46</b>	
<b>Troubleshooting.....</b>	<b>377</b>
46.1 Power, Hardware Connections, and LEDs .....	377
46.2 Switch Access and Login .....	378
46.3 Switch Configuration .....	380
<b>Chapter 47</b>	
<b>Product Specifications.....</b>	<b>381</b>
Appendix A Common Services .....	397
Appendix B Legal Information.....	401
<b>Index .....</b>	<b>403</b>



---

# PART I

## User's Guide

---



# Getting to Know Your Switch

This chapter introduces the main features and applications of the Switch.

## 1.1 Introduction

The Switch is a stand-alone layer-2 VDSL over Ethernet switch with one Telco-50 connector for VDSL connections and another for POTS connections. The switch also comes with one 10/100Base-TX Ethernet management port, two Gigabit/mini-GBIC uplink ports and a console management port.

With its built-in Web Configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

See [Chapter 47 on page 381](#) for a full list of software features available on the Switch.

This section shows a few examples of using the Switch in various network environments.

## 1.2 Applications

These are the main applications for the switch:

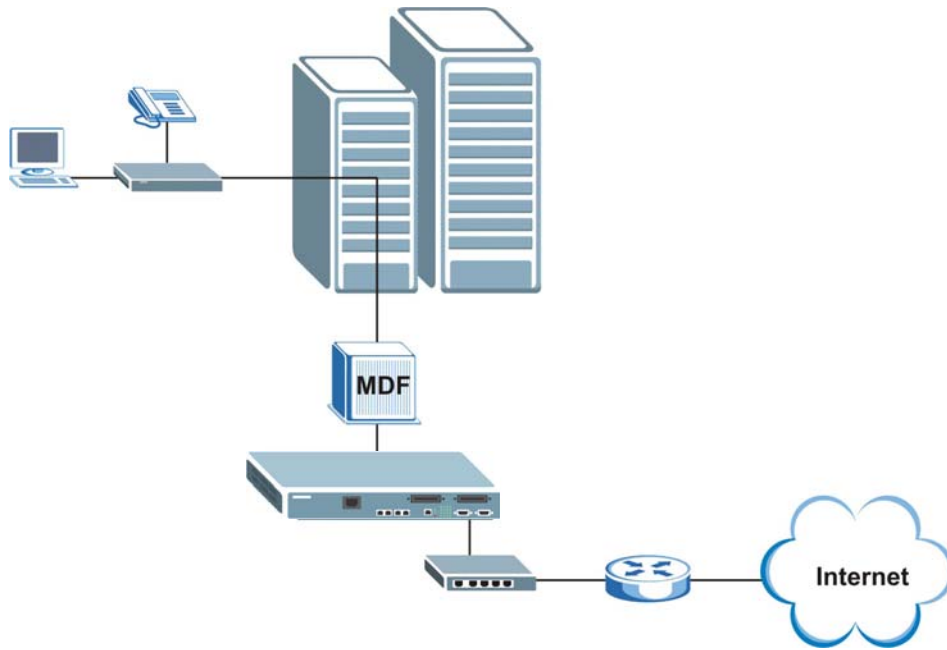
- Internet access and multimedia services for Multiple Tenant Units (MTU).
- Other applications include telemedicine, surveillance systems, remote servers systems, cellular base stations and high-quality teleconferencing.

### 1.2.1 MTU Application

The following diagram depicts a typical application of the switch with the VDSL modems, in a large residential building, or multiple tenant unit (MTU), that leverages existing phone line wiring to

provide Internet access to all tenants. Note that VDSL service can coexist with voice service on the same line.

**Figure 1** MTU Application

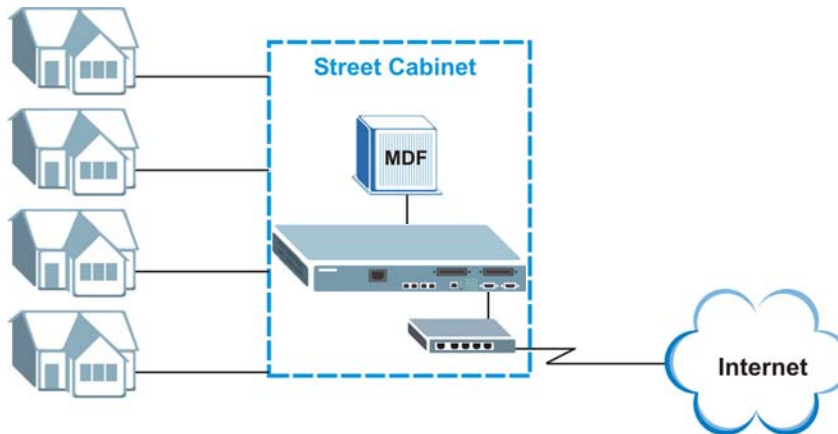


## 1.2.2 Curbside Application

The switch can also be used by an Internet Service Provider (ISP) in a street cabinet to form a “mini POP (Point-of-Presence)” to provide broadband services to residential areas that are too far away

from the ISP to avail of DSL services. Residents need a VDSL modem connected as shown in the previous figure.

**Figure 2** Curbside Application



## 1.3 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See [Chapter 4 on page 33](#).
- Command Line Interface. Line commands offer an alternative to the Web Configurator and in some cases are necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use FTP for firmware upgrades and configuration backup/restore. See [Section 36.8 on page 331](#).
- SNMP. The Switch can be monitored by an SNMP manager. See [Section 37.3 on page 334](#).

## 1.4 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.



# Hardware Installation and Connection

This chapter shows you how to install and connect the Switch.

## 2.1 Installation Scenarios

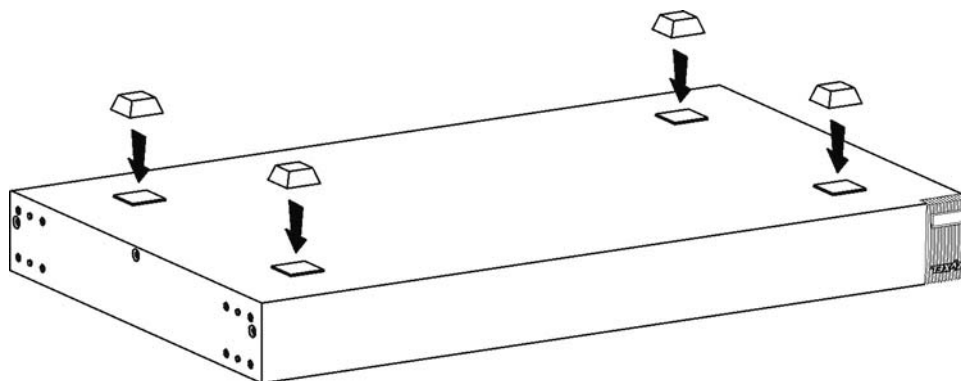
The Switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

Note: For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. Reserve at least 1.5U space above and below the Switch. This is especially important for enclosed rack installations.

## 2.2 Desktop Installation Procedure

- 1 Make sure the Switch is clean and dry.
- 2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.
- 3 Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.
- 4 Remove the adhesive backing from the rubber feet.
- 5 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

**Figure 3** Attaching Rubber Feet



Note: Do NOT block the ventilation holes. Leave space between devices when stacking.

## 2.3 Mounting the Switch on a Rack

The Switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your Switch on a standard EIA rack using a rack-mounting kit.

### 2.3.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

**Failure to use the proper screws may damage the unit.**

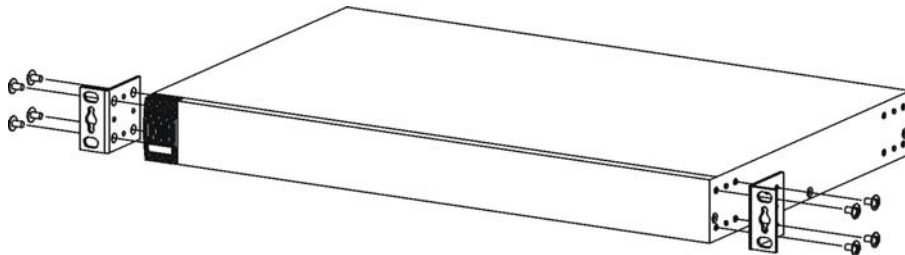
#### 2.3.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

### 2.3.2 Attaching the Mounting Brackets to the Switch

- 1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

**Figure 4** Attaching the Mounting Brackets



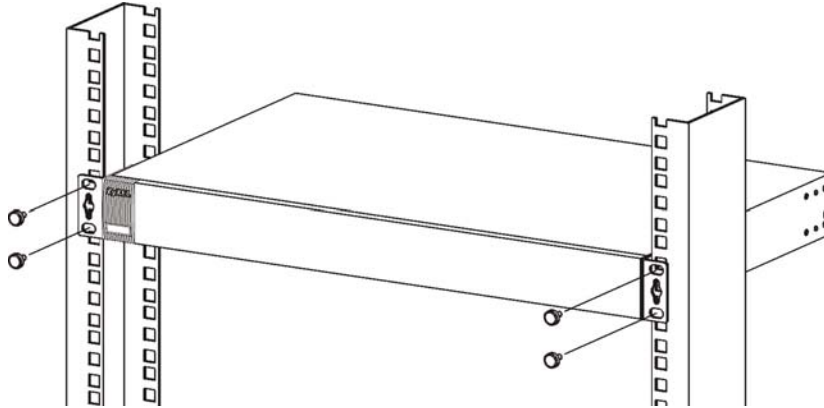
- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.
- 4 You may now mount the Switch on a rack. Proceed to the next section.



### 2.3.3 Mounting the Switch on a Rack

- 1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

**Figure 5** Mounting the Switch on a Rack



- 2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.
- 3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

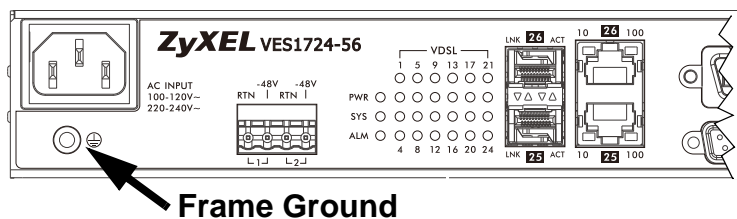
## 2.4 Connecting the Frame Ground

Connect the frame ground on the front panel using an M4 x 6mm machine screw with 2 suitable lock washers to a building's protective earthing terminals.

**Use a 18 AWG or larger green-and-yellow frame ground wire.**

**Connect the frame ground before you connect any other cables or wiring.**

**Figure 6** Frame Ground



## Hardware Overview

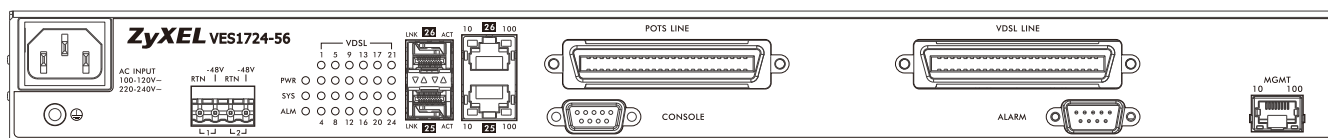
This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

**To protect yourself from the Switch's high operating temperatures, wear protective gloves before you touch the Switch.**

### 3.1 Front Panel

The following figure shows the front panel of the Switch.

**Figure 7** Front Panel



The following table describes the port labels on the front panel.

**Table 1** Front Panel Connections

LABEL	DESCRIPTION
Power Connection	Connect an appropriate power supply to one and only one of the ports.
Two Dual Personality Interfaces (25, 26)	<p>Each interface has one 1000 Base-T copper RJ-45 port and one mini-GBIC slot, with one port active at a time.</p> <ul style="list-style-type: none"> <li>100/1000 Mbps RJ-45 GbE Ports: Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches.</li> <li>Mini-GBIC Slots: Use mini-GBIC transceivers in these slots for fiber-optic or copper connections to backbone Ethernet switches.</li> </ul>
POTS LINE	This Telco-50 port connect to the central office or a PBX .
CONSOLE	The console port is for local configuration of the Switch.
VDSL LINE	This Telco-50 port connect to the user (subscriber) VDSL equipment.
ALARM	This port is for alarm.
MGMT	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the Switch.

#### 3.1.1 Power Connector

Note: Make sure you are using the correct power source as shown on the panel.

To connect power to the Switch, insert the female end of the power cord to either the AC or DC power receptacle on the front panel, depending on your power source. Connect the other end of the supplied power cord to a power outlet.

The dual power connector model has both AC and DC power connectors. See Figure 7. In this model,

- for the AC power connection, use AC power supply input of 100 VAC to 120 VAC with 50/60 Hz  $\pm$  3 Hz, 1.4 A maximum no tolerance or 220 VAC to 240 VAC with 50/60Hz  $\pm$  3 Hz, 1 A maximum no tolerance.
- for the DC power connection, use DC power supply input of -36 VDC to -72 VDC, 2 A maximum no tolerance.

Note: Do NOT make both AC and DC power connections at the same time. Turn the DC power off if you are using the AC power connection or are not using the device. Disconnect the AC power before you install the DC power module.

See [Chapter 47 on page 381](#) for information on the Switch's power supply requirements.

## 3.1.2 Gigabit Ethernet Ports

The Switch has 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 10/100/1000 Mbps Fast Ethernet, the speed can be 10 Mbps, 100 Mbps or 1000 Mbps and the duplex mode can be half duplex or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Two of the 1000Base-T Ethernet ports are paired with a mini-GBIC slot to create a dual personality interface. The Switch uses up to one connection for each mini-GBIC and 1000Base-T Ethernet pair. The mini-GBIC slots have priority over the Gigabit ports. This means that if a mini-GBIC slot and the corresponding GbE port are connected at the same time, the GbE port will be disabled.

When auto-negotiation is turned on, a Ethernet port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

### 3.1.2.1 Default Ethernet Negotiation Settings

The factory default negotiation settings for the Gigabit ports on the Switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

### 3.1.2.2 Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

### 3.1.3 Mini-GBIC Slots

These are slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic or even copper cable connectors.

**To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.**

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

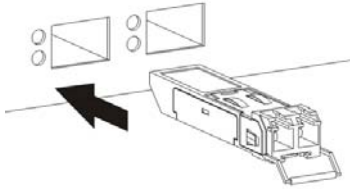
#### 3.1.3.1 Transceiver Installation

Use the following steps to install a mini-GBIC transceiver (SFP module).

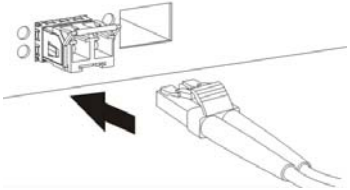
- 1 Insert the transceiver into the slot with the exposed section of PCB board facing down.
- 2 Press the transceiver firmly until it clicks into place.
- 3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
- 4 Close the transceiver's latch (latch styles vary).

- 5 Connect the fiber optic cables to the transceiver.

**Figure 8** Transceiver Installation Example



**Figure 9** Connecting the Fiber Optic Cables

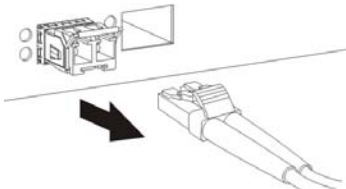


### 3.1.3.2 Transceiver Removal

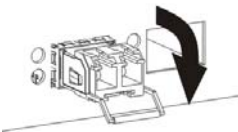
Use the following steps to remove a mini-GBIC transceiver (SFP module).

- 1 Remove the fiber optic cables from the transceiver.
- 2 Open the transceiver's latch (latch styles vary).
- 3 Pull the transceiver out of the slot.

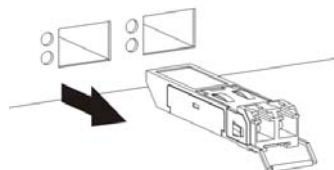
**Figure 10** Removing the Fiber Optic Cables



**Figure 11** Opening the Transceiver's Latch Example



**Figure 12** Transceiver Removal Example



### 3.1.4 Management Port

The **MGMT** (management) port is used for local management. Connect directly to this port using an Ethernet cable. You can configure the Switch via Telnet or the Web Configurator.

The default IP address of the management port is 192.168.0.1 with a subnet mask of 255.255.255.0.

### 3.1.5 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

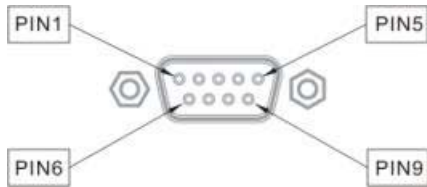
- VT100
- Terminal emulation
- 115200 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

### 3.1.6 ALARM Slot

The ALARM port is a male 9-pin connector. The following figure shows the pin assignments.

**Figure 13** Alarm Port: Pin Assignment



The following table describes the alarm pins.

**Table 2** Alarm Port: Pin Assignment

ALARM INPUT	PIN	DESCRIPTION
1	Pin 2 and Pin 6	An open circuit for pins 2 and 6 indicates no alarm status. A closed circuit indicates an alarm status.
2	Pin 3 and Pin 7	An open circuit for pins 3 and 7 indicates no alarm status. A closed circuit indicates an alarm status.
3	Pin 4 and Pin 8	An open circuit for pins 4 and 8 indicates no alarm status. A closed circuit indicates an alarm status.
4	Pin 5 and Pin 9	An open circuit for pins 5 and 9 indicates no alarm status. A closed circuit indicates an alarm status.

## 3.2 LEDs

After you connect the power to the Switch, view the LEDs to ensure proper functioning of the Switch and as an aid in troubleshooting.

**Table 3** LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	On	The system is on and functioning properly.
		Blinking	The system is rebooting and performing self-diagnostic tests.
	Off	The power is off or the system is not ready/malfunctioning.	
ALM	Red	On	A hardware failure is detected, or an external alarm is active.
		Off	The system is functioning normally.
Ethernet Ports			
LNK/ACT	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		On	The link to a 10 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
	Off	The link to an Ethernet network is down.	
Mini-GBIC Slots			
LNK	Green	On	The link to this port is up.
		Off	The link to this port is not connected.
ACT	Green	Blinking	This port is receiving or transmitting data.
1000Base-T Ethernet Ports (in Dual Personality Interface)			
LNK/ACT	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		On	The link to a 10 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
	Amber + Green	Blinking	The system is transmitting/receiving to/from a 1000 Mbps Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
	Off	The link to an Ethernet network is down.	
FDX	Amber	On	The Gigabit port is negotiating in full-duplex mode.
		Off	The Gigabit port is negotiating in half-duplex mode.
MGMT			
10	Green	Blinking	The system is transmitting/receiving to/from an Ethernet device.
		On	The port is connected at 10 Mbps.
	Off	The port is not connected at 10 Mbps or to an Ethernet device.	

**Table 3** LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
100	Amber	Blinking	The system is transmitting/receiving to/from an Ethernet device.
		On	The port is connected at 100 Mbps.
		Off	The port is not connected at 100 Mbps or to an Ethernet device.



# The Web Configurator

This section introduces the configuration and functions of the Web Configurator.

## 4.1 Introduction

The Web Configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 8 or Mozilla Firefox 6.0.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

## 4.2 System Login

- 1 Configure your computer's IP address in the same network as the Switch's management port. (For example, 192.168.0.x/24)
- 2 Start your web browser.
- 3 Type "http://" and the IP address of the Switch (for example, the default management IP address is 192.168.0.1 through the **MGMT** port) in the **Location** or **Address** field. Press [ENTER].
- 4 The login screen appears. The default username is **admin** and associated default password is **1234**.

Note: Alternatively, you can log into the Web Configurator through an in-band (non-MGMT) port. The default in-band management IP address is 192.168.1.1.

**Figure 14** Web Configurator: Login



- 5 Click **OK** to view the first Web Configurator screen.

## 4.3 The Port Status Screen

The **Port Status** screen is the first screen that displays when you access the Web Configurator.

The following figure shows the navigating components of a Web Configurator screen.

**Figure 15** Web Configurator Home Screen (Port Status)

The screenshot shows the ZyXEL Web Configurator interface. On the left is a 'MENU' sidebar with items: Basic Setting, VDSL Setup, Advanced Application, IP Application, and Management. Callout 'A' points to the 'VDSL Setup' item. At the top right are five callouts: 'B' points to a 'Save' button, 'C' to a 'Status' button, 'D' to a 'Logout' button, and 'E' to a 'Help' button. The main content area is titled 'Port Status' and contains a table with columns: Port, Name, Link, State, LACP, TxPkts, RxPkts, Errors, Tx KB/s, Rx KB/s, Up Time, and Retrain. The table lists 15 ports, all with 'Handshake' state and '0' for various counters. Below the table are radio buttons for 'Any' and 'Port', and a 'Clear Counter' button. The footer contains the copyright notice: '© Copyright 1995-2011 by ZYXEL Communications Corp.'

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time	Retrain
1		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
2		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
3		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
4		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
5		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
6		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
7		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
8		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
9		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
10		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
11		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
12		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
13		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
14		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain
15		0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain

**A** - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

**B, C, D, E** - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

**B** - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

**C** - Click this link to go to the status page of the Switch.

**D** - Click this link to logout of the Web Configurator.

**E** - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

**Table 4** Navigation Panel Sub-links Overview

BASIC SETTING	VDSL SETUP	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
<ul style="list-style-type: none"> <li>System Info</li> <li>General Setup</li> <li>Switch Setup</li> <li>IP Setup</li> <li>External Alarm Switch</li> <li>Port Setup</li> <li>Rate Limit Profile Setup</li> <li>Hardware Alarm Profile</li> <li>CPE Port Status</li> <li>IPv6 Setup</li> <li>SFP Threshold Setup</li> </ul>	<ul style="list-style-type: none"> <li>VDSL Line Setup</li> <li>VDSL Profile</li> <li>VDSL Alarm Profile</li> <li>VDSL Bonding Setup</li> </ul>	<ul style="list-style-type: none"> <li>VLAN</li> <li>Static MAC Forwarding</li> <li>Static Multicast Forwarding</li> <li>Filtering</li> <li>Spanning Tree Protocol</li> <li>Broadcast Storm Control</li> <li>Mirroring</li> <li>Link Aggregation</li> <li>Port Authentication</li> <li>MAC Limit</li> <li>Classifier</li> <li>Policy Rule</li> <li>Queuing Method</li> <li>VLAN Stacking</li> <li>Multicast</li> <li>Auth and Acct</li> <li>IP Source Guard</li> <li>Loop Guard</li> <li>CFM</li> <li>VLAN Mapping</li> <li>Layer 2 Protocol Tunneling</li> <li>DoS Prevention</li> <li>PPPoE IA Configuration</li> <li>ADSL Fallback</li> </ul>	<ul style="list-style-type: none"> <li>Static Routing</li> <li>DiffServ</li> <li>DHCP</li> <li>DHCPv6 LDRA</li> </ul>	<ul style="list-style-type: none"> <li>Maintenance</li> <li>Access Control</li> <li>Diagnostic</li> <li>Syslog</li> <li>Loop Diagnostic</li> <li>MAC Table</li> <li>ARP Table</li> <li>Hardware Information</li> <li>CFM Action</li> <li>IPv6 Cache</li> </ul>

The following table describes the links in the navigation panel.

**Table 5** Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, MAC address learning, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the management IPv4/IPv6 address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 64 IPv4 routing domains.
External Alarm Switch	This link takes you to a screen where you can view the status of each external alarm input and configure their settings.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.
Rate Limit Profile Setup	This link takes you to screens where you can configure the ingress and egress rate limit profiles to apply to ports. You can use this setting in the <b>Basic Setting &gt; Port Setup</b> later.
Hardware Alarm Profile	This link takes you to a screen where you can configure alarm thresholds.
CPE Port Status	This link takes you to a screen where you can view all DSL port status and details about the connected CPE devices.
IPv6 Setup	This link takes you to a screen where you can configure the IPv6 settings.
SFP Threshold Setup	This link takes you to a screen where you can configure warning or alarm thresholds for the SFP slots of the Switch.

**Table 5** Navigation Panel Links (continued)

LINK	DESCRIPTION
VDSL Setup	
VDSL Line Setup	This link takes you to a screen where you can assign a VDSL template, VDSL fallback template, and VDSL alarm template for each VDSL port.
VDSL Profile	This link takes you to screens where you can create, modify and delete VDSL templates, VDSL line profiles, VDSL channel profiles and VDSL INM profiles. A VDSL template contains a VDSL line profile, a VDSL channel profile and a VDSL INM profile.
VDSL Alarm Profile	This link takes you to screens where you can create, modify and delete VDSL alarm templates, VDSL line alarm profiles and VDSL channel alarm profiles. A VDSL alarm template contains a VDSL line alarm profile and a VDSL channel alarm profile.
VDSL Bonding Setup	This link takes you to a screen where you can configure VDSL port bonding that increases the total bandwidth for subscribers by combining two DSL lines.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the <b>Switch Setup</b> menu). You can also configure a protocol based VLAN, a subnet based VLAN or a MAC based VLAN in these screens.
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the Switch.
MAC Limit	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port and/or in a VLAN.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to a screen where you can configure VLAN stacking.
Multicast	This link takes you to screens where you can configure various multicast features, IGMP snooping and create multicast VLANs.
Auth and Acct	This link takes you to a screen where you can configure authentication and accounting service via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.

**Table 5** Navigation Panel Links (continued)

LINK	DESCRIPTION
CFM	This link takes you to screens where you can configure Connectivity Fault Management (CFM), MD (maintenance domain), and MA (maintenance association).
VLAN Mapping	This link takes you to screens where you can configure VLAN mapping settings on the Switch.
Layer 2 Protocol Tunneling	This link takes you to a screen where you can configure L2PT (Layer 2 Protocol Tunneling) settings on the Switch.
DoS Prevention	This link takes you to a screen where you can configure filtering actions on the Switch to determine when to drop packets that may potentially be associated with a DoS attack.
PPPoE IA Configuration	This link takes you to screens where you can configure how the Switch gives a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.
ADSL Fallback	This link takes you to a screen where you can configure PVC settings for individual DSL ports, which are applied when the Switch falls back to use ADSL/ADSL2/ADSL2+ on a DSL line.
IP Application	
Static Routing	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
DHCPv6 LDRA	This link takes you to screens where you can configure the Lightweight DHCPv6 Relay Agent (LDRA) settings.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to a screen where you can view system logs and test port(s).
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Loop Diagnostic	This link takes you to a screen where you can perform single-end loop test (SELT) and dual-end loop test (DELT) for each port.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Hardware Information	This link takes you to a screen where you can check hardware detailed information such as CPU, packet buffer, memory utilization.
CFM Action	This link takes you to a screen where you can perform connectivity tests and see testing reports.
IPv6 Cache	This link takes you to screens where you can view IPv6 caches.

### 4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management** > **Access Control** > **Logins** to display the next screen.

**Figure 16** Change Administrator Login Password

**Logins** [Access Control](#)

**Administrator**

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

**Edit Logins**

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

## 4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right hand corner of the Web Configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

Note: Use the **Save** link when you are done with a configuration session.

## 4.5 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) if you do one of the following:

- 1 Delete the management VLAN (default is VLAN 1).
- 2 Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
- 3 Filter all traffic to the CPU port.

- 4 Disable all ports.
- 5 Misconfigure the text configuration file.
- 6 Forget the password and/or IP address.
- 7 Prevent all services from accessing the Switch.
- 8 Change a service port number but forget it.

Note: Be careful not to lock yourself and others out of the Switch. If you do lock yourself out, try using out-of-band management (via the management port) to configure the Switch.

## 4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

### 4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 115200 bps with 8 data bits, no parity, one stop bit and flow control set to none. The password will also be reset to "1234" and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

- 1 Connect to the console port using a computer with terminal emulation software.
- 2 Disconnect and reconnect the Switch's power to begin a session. When you reconnect the Switch's power, you will see the initial screen.
- 3 When you see the message "Press any key to enter Debug Mode within 3 seconds ..." press any key to enter debug mode.
- 4 Type `atlc` after the "Enter Debug Mode" message.
- 5 Wait for the "Starting XMODEM upload" message before activating XMODEM upload on your terminal.



- 6 After a configuration file upload, type `atgo` to restart the Switch.

**Figure 17** Resetting the Switch: Via the Console Port

```

Bootbase Version: V56Fanless | 10/23/2012 11:00:25
RAM: Size = 131072 Kbytes
DRAM POST: Testing: 23488K
OK
FLASH: AMD 128M *1

ZyNOS Version: V56_Fanless130626 | 06/26/2013 10:21:50

Press any key to enter debug mode within 3 seconds.
ras> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 393216 bytes received.
Erasing..
.....
OK
ras> atgo

```

The Switch is now reinitialized with a default configuration file including the default password of "1234".

## 4.7 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the Web Configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

**Figure 18** Web Configurator: Logout Screen



## 4.8 Help

The Web Configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a Web Configurator screen to view an online help description of that screen.

# Initial Setup Example

This chapter shows how to set up the Switch for an example network.

## 5.1 Overview

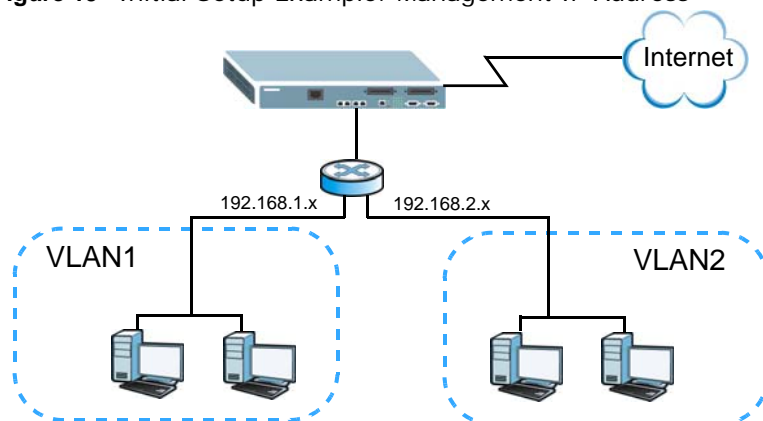
The following lists the configuration steps for the initial setup:

- Configure the Switch IP management address
- Create a VLAN
- Set port VLAN ID

## 5.2 Configuring Switch Management IP Address

The default management IP address of the Switch is 192.168.1.1. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

**Figure 19** Initial Setup Example: Management IP Address



- 1 Connect your computer to an in-band Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.
- 2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the Web Configurator. See [Section 4.2 on page 33](#) for more information.

- 3 Click **Basic Setting** > **IP Setup** in the navigation panel.
- 4 Configure the related fields in the **IP Setup** screen.
- 5 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.
- 6 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 7 Click **Add** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

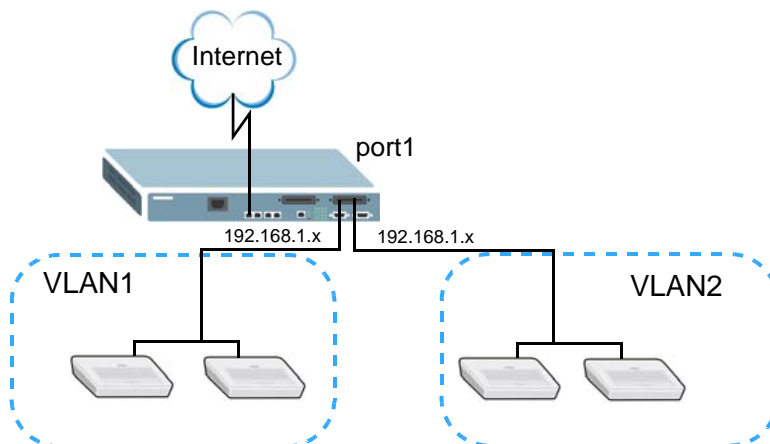
The screenshot shows the 'IP Setup' configuration interface. At the top, 'Domain Name Server' is set to 0.0.0.0 and 'Default Management' is set to 'In-band'. Under 'In-band Management IP Address', the 'Static IP Address' option is selected and highlighted with a red circle. It shows: IP Address: 192.168.2.1, IP Subnet Mask: 255.255.255.0, Default Gateway: 0.0.0.0, and VID: 2. Below this, 'Out-of-band Management IP Address' is configured with IP Address: 192.168.0.1, IP Subnet Mask: 255.255.255.0, and Default Gateway: 0.0.0.0. At the bottom, the 'In-band IP Addresses (VPS)' section is visible with fields for IP Address (VPS), IP Subnet Mask, VID, Default Gateway, and a 'Manageable' checkbox. 'Add' and 'Cancel' buttons are present at the bottom of the form.

## 5.2.1 Creating a VLAN

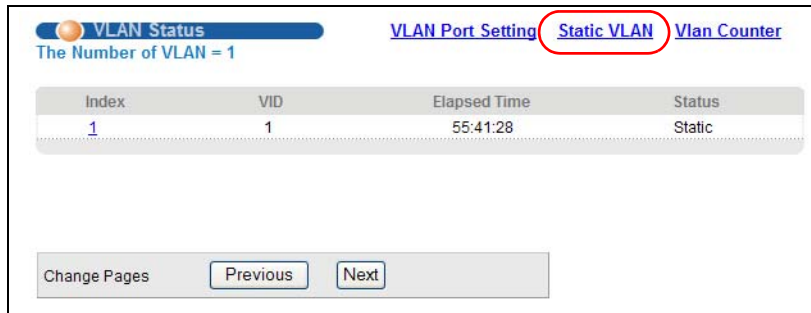
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 and port 2 as members of VLAN 2.

**Figure 20** Initial Setup Network Example: VLAN



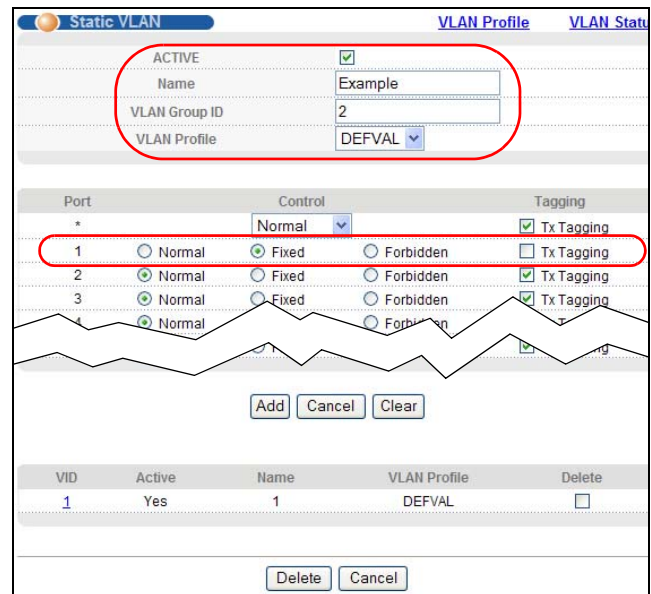
- 1 Click **Advanced Application** > **VLAN** in the navigation panel and click the **Static VLAN** link.



- 2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.

Note: The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

- 3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
- 4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.



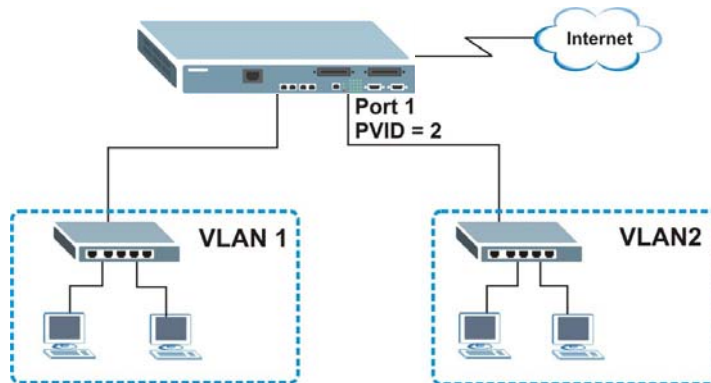
- 5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

## 5.2.2 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

**Figure 21** Initial Setup Network Example: Port VID



- 1 Click **Advanced Application** > **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.
- 2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

VLAN Port Setting					
<a href="#">Subnet Based Vlan</a> <a href="#">Protocol Based Vlan</a> <a href="#">VLAN Status</a>					
GVRP <input type="checkbox"/>					
Port isolation <input type="checkbox"/>					
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>
1	<input type="checkbox"/>	2	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
10	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

This chapter provides some examples of using the Web Configurator to set up and use the Switch. The tutorial describes:

- [How to Use DHCP Relay Per VLAN on the Switch](#)

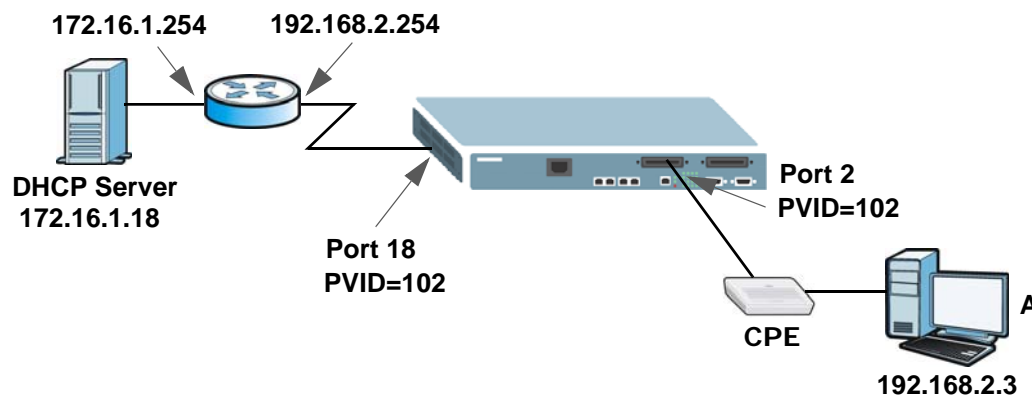
## 6.1 How to Use DHCP Relay Per VLAN on the Switch

This tutorial describes how to configure your Switch to forward DHCP client requests from a client to a DHCP server in a specific VLAN. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

### 6.1.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (say 172.16.1.18) and want to have it assign a specific IP address (say 192.168.2.3) to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the Switch's port 2 and the DHCP server connects to port 18. Both port 2 and port 18 are in VLAN 102.

**Figure 22** Tutorial: DHCP Relay Per VLAN Scenario



### 6.1.2 Creating a VLAN

Follow the steps below to configure ports 2 and 18 as a member of VLAN 102.

- 1 Access the Web Configurator through the Switch's management port.

- Go to **Basic Setting > Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.

**Figure 23** Tutorial: Set VLAN Type to 802.1Q

**Switch Setup**

VLAN Type:  802.1Q  Port Based

Bridge Control Protocol Transparency: Active

MAC Address Learning: Aging Time: 300 seconds

Join Timer: 200 milliseconds

GARP Timer: Leave Timer: 600 milliseconds

Leave All Timer: 10000 milliseconds

Priority Queue Assignment:

level7	7
level6	6
level5	5
level4	4
level3	3
level2	1
level1	0
level0	2

Apply Cancel

- Click **Advanced Application > VLAN > Static VLAN**.
- In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 102 for example) in the **Name** field and enter 102 in the **VLAN Group ID** field.
- Select **Fixed** to configure ports 2 and 18 to be a permanent member of this VLAN. To ensure the VLAN-unaware devices, such as computers can receive frames properly, clear the **Tx Tagging** check box for port 2 to have the Switch remove VLAN tags before sending. Click **Add**.

**Figure 24** Tutorial: Create a Static VLAN

**Static VLAN** [VLAN Profile](#) [VLAN Status](#)

ACTIVE

Name: VLAN 102

VLAN Group ID: 102

VLAN Profile: DEFVAL

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
18	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

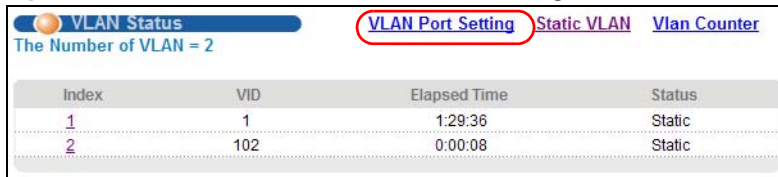
Add Cancel Clear

VID	Active	Name	VLAN Profile	Delete
1	Yes	1	DEFVAL	<input type="checkbox"/>

Delete Cancel

- Click the **VLAN Status** link in the **Static VLAN** screen and then the **VLAN Port Setting** link in the **VLAN Status** screen.

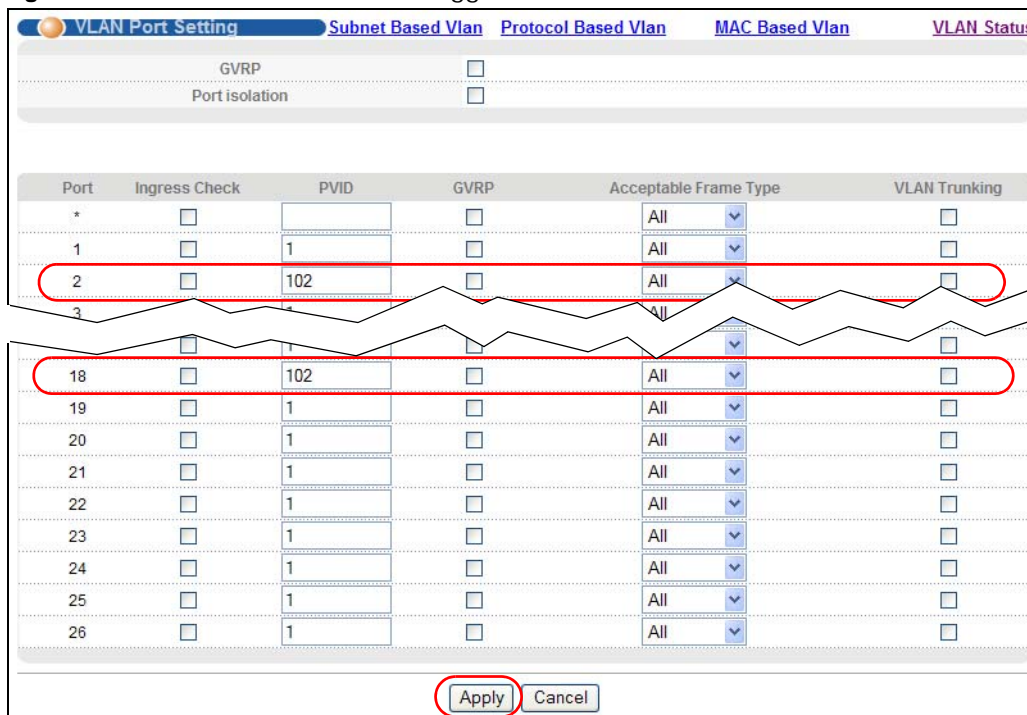
**Figure 25** Tutorial: Click the VLAN Port Setting Link



Index	VID	Elapsed Time	Status
1	1	1:29:36	Static
2	102	0:00:08	Static

- Enter 102 in the **PVID** field for ports 2 and 18 to add a tag to incoming untagged frames received on these ports so that the frames are forwarded to the VLAN group that the tag defines. Click **Apply**.

**Figure 26** Tutorial: Set PVID for untagged frames received on Ports 2 and 18



Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	102	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
10	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
11	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
12	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
13	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
14	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
15	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
16	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
17	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
18	<input type="checkbox"/>	102	<input type="checkbox"/>	All	<input type="checkbox"/>
19	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
20	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
21	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
24	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
25	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
26	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

- Click the **Save** link in the upper right corner of the Web Configurator to save your configuration permanently.

### 6.1.3 Configuring Management IP Address

Follow the steps below to specify a management IP address for VLAN 102 and the IP address of the default gateway, an IEEE 802.1Q VLAN-aware layer-3 switch or router that helps forward DHCP packets to the DHCP server.

- Click **Basic Setting > IP Setup**.
- For the VLAN 102 network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.



- 3 In the **VID** field, enter the ID of the VLAN group (102 in this example) to which you want this management IP address to belong.
- 4 Enter the IP address of the default gateway (192.168.2.254 for example) in the **Default Gateway** field.
- 5 Click **Add**.

**Figure 27** Tutorial: Set Management IP Address for VLAN 102

**IP Setup**

Domain Name Server: 0.0.0.0

Default Management:  In-band  Out-of-band

**In-band Management IP Address**

DHCP Client

DHCP Option 12: DSLAM VES1724-4

DHCP Option 60: DSLAM cc5d-4e00

Static IP Address

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

VID: 1

**Out-of-band Management IP**

IP Address: 192.168.0.1

Apply Cancel

**In-band IP Addresses (VPS)**

Index	IP Address (VPS)	IP Subnet Mask	VID	Default Gateway	Manageable	Delete
	192.168.2.1	255.255.255.0	102	192.168.2.254	<input type="checkbox"/>	

Add Cancel

Delete Cancel

- 6 Click the **Save** link in the upper right corner of the Web Configurator to save your configuration permanently.

### 6.1.4 Configuring DHCP VLAN Settings

Follow the steps below to have the Switch act as a DHCP relay agent for the specified VLAN and allow the Switch to add relay agent information (such as the VLAN ID) to DHCP requests.

Note: Make sure you have disabled global DHCP relay in the **IP Application > DHCP > Global** screen before you configure DHCP relay per VLAN settings.

- 1 Click **IP Application > DHCP** and then the **VLAN** link to open the **VLAN Setting** screen.
- 2 Enter 102 in the **VID** field.
- 3 Enter the DHCP server's IP address (172.16.1.18 in this example) in the **Remote DHCP Server 1** field.
- 4 Select **Option 82** and enter the Switch's model name in the **Information** field.
- 5 Leave the **Relay Remote ID** and **Remote ID Information** fields empty unless something needs to be specified.
- 6 Click **Add**.

**Figure 28** Tutorial: Set DHCP Server and Relay Information

VID	102
Remote DHCP Server 1	172.16.1.18
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	<input checked="" type="checkbox"/> Option 82 <input type="checkbox"/> Swap position of Circuit ID and Remote ID
Tag Option	private
Delimiter	none
Information	<input checked="" type="radio"/> VES <input type="radio"/> Append Circuit ID by host name
Relay Remote ID	<input type="checkbox"/> Remote ID <input checked="" type="radio"/> Append Remote ID by user identifier
Remote ID Information	<input type="radio"/> Append Remote ID by port name <input type="radio"/> Append Remote ID by user identifier + port name + port TEL
Remote ID user identifier	
Remote ID Delimiter	

- 7 Click the **Save** link in the upper right corner of the Web Configurator to save your configuration permanently.
- 8 The Switch can then forward the DHCP packets between the clients and DHCP server in VLAN 102.

### 6.1.5 Testing the Connection

Check the client **A**'s IP address. If it did not receive the IP address 192.168.2.3, make sure the devices are connected and configured properly.

---

# PART II

## Technical Reference

---



# System Status and Port Statistics

This chapter describes the system status (Web Configurator home page) and port details screens.

## 7.1 Overview

The home screen of the Web Configurator displays a port statistical summary with links to each port showing statistical details.

## 7.2 Port Status Summary

To view the port statistics, click **Status** in all Web Configurator screens to display the **Status** screen as shown next.

**Figure 29** Port Status

Port Status													VDSL Summary	
Port	Name	Group	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time	Retrain		
<a href="#">1</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">2</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">3</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">4</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">5</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">6</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">7</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">8</a>			0/0	Handshake	-	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">25</a>			Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	Retrain		
<a href="#">26</a>			Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	Retrain		

Any  
 Port

The following table describes the labels in this screen.

**Table 6** Port Status

LABEL	DESCRIPTION
Port	This identifies a VDSL or Ethernet port. Click a port number to display the <b>Port Details</b> screen (refer to <a href="#">Figure 35 on page 67</a> ).
Name	This is the name you assigned to this port in the <b>Basic Setting &gt; Port Setup</b> screen.
Group	This is the name of the VDSL port bonding group if the port is a member of one. Click the link to view more information about the group.

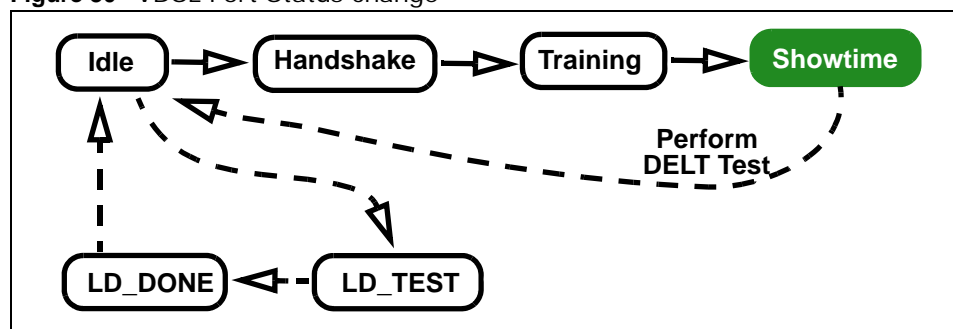
**Table 6** Port Status (continued)

LABEL	DESCRIPTION
Link	For an Ethernet port, this field displays the speed (either <b>10M</b> for 10Mbps, <b>100M</b> for 100Mbps or <b>1000M</b> for 1000Mbps) and the duplex ( <b>F</b> for full duplex or <b>H</b> for half). It also shows the cable type ( <b>Copper</b> or <b>Fiber</b> ) for the combo ports.  For a VDSL port, this field displays the VDSL transmission rate on the port.
State	For VDSL ports, this field displays <b>Showtime</b> when the VDSL connection is up. Otherwise, it displays <b>Idle</b> , <b>Handshake</b> or <b>Training</b> during the VDSL line establishment. If you perform a DELT test, this field will display <b>LD_Testing</b> or <b>LD_DONE</b> . See <a href="#">Section 7.2.1 on page 54</a> for more information.  For Ethernet ports, if STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see <a href="#">Section 14.1 on page 160</a> for more information). If STP is disabled, this field displays <b>FORWARDING</b> if the link is up, otherwise, it displays <b>STOP</b> .
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Retrain	Click <b>Retrain</b> to re-establish the line connection.
Clear Counter	Select <b>Port</b> , enter a port number and then click <b>Clear Counter</b> to erase the recorded statistical information for that port, or select <b>Any</b> to clear statistics for all ports.

## 7.2.1 VDSL Port Status Change

The VDSL port status change is shown as the following flow chart. Only when the status is "Showtime", the VDSL connection is up.

Note: It's suggested to perform the Dual-End-Loop-Test (DELT) when there is bad line quality even though the VDSL connection is up. It brings the connection down right away and takes several minutes to complete the whole test before re-negotiating the connection.

**Figure 30** VDSL Port Status change

## 7.2.2 VDSL Port Details

Click a VDSL port's index number in the **Port** column of the **Port Status** screen to display individual port statistics. Use this screen to check status and detailed performance data for an individual port on the Switch.

Note: This screen refreshes automatically every several minutes if the port is in any status other than in "Showtime".

Figure 31 Status: VDSL Port Details

VDSL Port Details		Port Details	
Port Info	Number	Port 1	
	Name	---	
	Link Type	---	
	State	Handshake	
	Up Time	0:00:00	
	Actual Template	DEFVAL	
	Transmission System	NONE	
	Init Result	noPeerAtu	
	Limit Mask	D-32	
	US0 Mask	EU-32	
	Electrical Length	0.0 dB	
	Cyclic Extension	5	

VDSL status	Items	Up Stream	Down Stream
	Attainable net data rate	0.000Mbps	0.000Mbps
	SNR Margin	0.0dB	0.0dB
	Signal Attenuation	0.0dB	0.0dB
	Line Attenuation	0.0dB	0.0dB
	Transmit Power	0.0dBm	0.0dBm
	Trellis	false	false
	Snr Mode	disable	disable
	Last State		
	Current State	lossOfSignal	lossOfSignal
	Actual net data rate	0.000Mbps	0.000Mbps
	Prev net data rate	0.000Mbps	0.000Mbps
	Actual Delay	0.0ms	0.0ms
	Actual INP	0.0symbols	0.0symbols
	Receive Power	0.0dBm	0.0dBm
	INP Report	Formula	Formula
	Codeword Size	0 bytes	0 bytes
	RFEC	0 bytes	0 bytes
	LSYMB	0 bits	0 bits
	Interleaving Depth	0	0
	Interleaving Block	0	0
	Actual Latency Path	0	0
	Ptm Status	noDefect	noDefect
	Actual RA Mode	n/a	n/a
	Retransmission Mode	n/a	n/a
	G.INP Framing Type	0	0
	Actual INP against REIN	0 symbols	0 symbols
	RS CW per DTU	0	0

VDSL Band Status	U0	U1	U2	U3	U4	D1	D2	D3	D4
SNR margin	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Signal Attenuation	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Line Attenuation	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Transmit Power	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Receive Power	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

VDSL Performance	Since Link		Curr 15 Min		Curr 1 Day	
Full Inits	---		0		0	
Failed Full Inits	---		0		0	
	Vtuc	Vtur	Vtuc	Vtur	Vtuc	Vtur
FECS	0	0	0	0	0	0
ES	0	0	0	0	0	0
SES	0	0	0	0	0	0



LOSs	0	0	0	0	0	0
LOFs	0	0	0	0	0	0
UAS	102593	0	894	0	16194	0
Code Violation	0	0	0	0	0	0
Corrected	0	0	0	0	0	0
Uncorrected	0	0	0	0	0	0
Rtx	0	0	0	0	0	0
RtxCorrected	0	0	0	0	0	0
RtxUncorrected	0	0	0	0	0	0
LEFTRs	0	0	0	0	0	0
MinEFTR	0	0	0	0	0	0
ErrFreeBits	0	0	0	0	0	0
LOLs/LOL	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
LPRs/LPR	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
Time Elapsed	0:00:00	0:00:00	113	113	16313	16313

VDSL Performance History  
[15 Min Interval](#)  
[One Day Interval](#)

VDSL INM PerformanceHistory  
[Current](#)  
[15 Min Interval](#)  
[One Day Interval](#)

VDSL sub-carrier status

Items	Direction	Display
Hlog	DownStream	Graph

Show Measure

MEDLEY PSD

Up Stream			Down Stream		
Break Point	Tone Index	PSD Level (dBm/Hz)	Break Point	Tone Index	PSD Level (dBm/Hz)
1	---	---	1	---	---
32	---	---	32	---	---
			33	---	---
			34	---	---
			35	---	---
			36	---	---
			37	---	---
			38	---	---
			39	---	---
			40	---	---
			41	---	---
			42	---	---
			43	---	---
			44	---	---
			45	---	---
			46	---	---
			47	---	---
			48	---	---

Poll Interval(s) 40 Set Interval Stop

The following table describes the labels in this screen.

**Table 7** Status: VDSL Port Details

LABEL	DESCRIPTION
Port Info	
Number	This field displays the selected port number.
Name	This field displays the descriptive name of the port.
Link Type	This field displays the type of the port.
State	This field displays whether the port is connected ( <b>Showtime</b> ), not connected ( <b>Idle</b> ), is searching for any CPE device ( <b>Handshake</b> ), is negotiating a connection with a CPE device ( <b>Training</b> ), is under loop diagnostic testing ( <b>LD_Testing</b> ), or has completed the loop diagnostic testing ( <b>LD_Done</b> ). See <a href="#">Section 7.2.1 on page 54</a> for more information.
Up Time	This field displays the total amount of time the line has been up.
Actual Template	This field displays the VDSL template the line is currently using.
Transmission System	This field displays the VDSL transmission mode the port is negotiating or has negotiated with the connected CPE device.
Init Result	This field displays the outcome of when the line was last initiated. The possible results are shown next.  <b>noFail</b> : The initialization was successful.  <b>configError</b> : The initialization failed because of a configuration error.  <b>configNotFeasible</b> : The initialization failed because a setting is not supported on both the Switch and the CPE.  <b>commFail</b> : The initialization failed because of a communication error between the Switch and the CPE.  <b>noPeerAtu</b> : The initialization failed because the Switch cannot detect the connected CPE device.  <b>otherCause</b> : The initialization failed because of another reason.
Limit Mask	To reduce the impact of interference and attenuation, ITU-T 993.2 specifies a limit PSD (Power Spectrum Density) mask that limits the VDSL2 transmitters' PSD for both downstream and upstream traffic.  This field displays a standard-defined limit PSD mask that the line is currently using.
US0 Mask	This field displays the PSD mask used for upstream band 0.  The possible masks are shown next. (See ITU-T G.993.2 Annex A for more information.)  <b>EU-32, EU-36, EU-40, EU-44, EU-48, EU-52, EU-56, EU-60, EU-64, EU-128</b>
Electrical Length	This field displays the final electrical length of the cable negotiated by the Switch and the connected CPE device. See <a href="#">UPBO/DPBO Electrical Length on page 100</a> .
Cyclic Extension	Cyclic extension is a method that adds a redundant data into each DMT symbol. This helps to reduce interference on a line.  This field displays the length of the redundant data used on the line.
VDSL Status	
Attainable net data rate	This parameter indicates the maximum upstream/downstream net data rate currently attainable by the Switch transmitter and the CPE receiver or by the CPE transmitter and the Switch receiver.
SNR Margin	This field displays the upstream/downstream SNR (Signal-to-Noise Rate) margin.
Signal Attenuation	This field displays the upstream/downstream loss of power (in dB) traveling along the line.

**Table 7** Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
Line Attenuation	<p>This field displays the upstream/downstream line attenuation the Switch detects according to the line length, frequency and the line wire diameter.</p> <p>Line attenuation increases with line length and frequency. Bigger wires reduce attenuation.</p>
Transmit Power	<p>This field displays the upstream/downstream transmission power of the line. It ranges from 0 to 25.5 dBm, with 0.1 dB steps for downstream. It ranges from 0 to 25.5 dBm, with 0.1 dB steps for upstream.</p>
Trellis	<p>This field displays whether trellis coding is used in the upstream/downstream transmission.</p>
Snr Mode	<p>This field displays whether the upstream/downstream transmitter referred virtual noise is enabled or disabled.</p>
Last State	<p>This field displays the last successful transmitted initialization state for upstream and downstream directions through the line. The possible states are as shown next.</p> <p><b>vtucG9941, vtucQuiet1, vtucChDiscov1, vtucSynchro1, vtucPilot1, vtucQuiet2, vtucPeriodic1, vtucSynchro2, vtucChDiscov2, vtucSynchro3, vtucTraining1, vtucSynchro4, vtucPilot2, vtucTeq, vtucEct, vtucPilot3, vtucPeriodic2, vtucTraining2, vtucSynchro5, vtucMedley, vtucSynchro6, vtucShowtime, vturG9941, vturQuiet1, vturChDiscov1, vturSynchro1, vturLineprobe, vturPeriodic1, vturSynchro2, vturChDiscov2, vturSynchro3, vturQuiet2, vturTraining1, vturSynchro4, vturTeq, vturQuiet3, vturEct, vturPeriodic2, vturTraining2, vturSynchro5, vturMedley, vturSynchro6, vturShowtime.</b></p>
Current State	<p>This field displays any existing upstream/downstream failure for the line.</p> <p><b>NoDefect:</b> No failure was detected.</p> <p><b>LossOfFraming:</b> A loss of frame synchronization was detected.</p> <p><b>LossOfSignal:</b> A loss of signal was detected.</p> <p><b>LossOfPower:</b> A loss of power was detected.</p> <p><b>InitFailure:</b> The most recent initialization failed.</p>
Actual net data rate	<p>This field displays the actual upstream/downstream data transmission rate.</p>
Prev net data rate	<p>This field displays the previous upstream/downstream data transmission rate just before the rate changed.</p>
Actual Delay	<p>This field displays the actual upstream/downstream interleave delay (in milliseconds) used on the line.</p>
Actual INP	<p>This field displays the actual impulse noise protection (INP).</p>
Receive Power	<p>This field displays the upstream/downstream receiving power of the line. The range is from 0 to 25.5 dBm with 0.1 dB steps for both downstream and upstream traffic.</p>
INP Report	<p>This field displays the method used to compute the actual INP above. <b>Formula</b> displays if the value is computed according to an INP_no_erasure formula defined in the ITU-T G.993.2 standard.</p>
Codeword Size	<p>This field displays the actual size of Reed-Solomon codeword used in this line. Reed-Solomon (RS) Code is an error-correction code.</p>
RFEC	<p>RFEC refers to Redundancy Forward Error Correction. This field displays the actual number of Reed-Solomon redundancy bytes. The Reed-Solomon code has the capability to correct errors by adding redundancy bytes. The longer the Reed-Solomon redundancy bytes the higher the error correction capability.</p>
LSYMB	<p>LSYMB refers to Latency SYMBol Bit. This field displays the actual number of bits per symbol.</p>

**Table 7** Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
Interleaving Depth	This field displays the actual interleaving depth. The value ranges from 1 to 4096 with an increment of 1. The value 1 indicates no interleaving.
Interleaving Block	This field displays the actual interleaving block length. The value ranges from 4 to 255 with an increment of 1.
Actual Latency Path	This field displays the ID of the channel the Switch is using for that port. All the following fields describe the status for this channel.
Ptm Status	<p>Packet Transfer Mode is a packet-based (for example, for Ethernet packets, IP packets, etc.) transmission method applied in VDSL2. It can highly increase the efficiency of packet transmission.</p> <p>This field displays the current state of the VDSL channel in packet transfer mode.</p> <p><b>noDefect:</b> means both Switch and CPE device did not detect any failure or the channel is not using packet transfer mode.</p> <p><b>outOfSync:</b> means an out of synchronization failure was detected.</p>
Actual RA Mode	<p>This field displays actual rate adaptive mode.</p> <p><b>n/a:</b> no CPE device is connected to this port.</p> <p><b>RA mode at init:</b> the Switch keeps the transmission rate negotiated between the Switch and CPE devices. It ranges from the configured minimum to the maximum net data rate (set in the <b>VDSL Setup &gt; VDSL Profile &gt; ChanProfile</b> screen) based on the initial line condition. The Switch automatically resumes a dropped link and adjusts the data rate back to the allowed range.</p> <p><b>Fixed rate mode:</b> the Switch fixes the transmission rate as the minimum net data rate and disables transmission rate adjustment. If the attainable speeds cannot match configured speeds, then the VDSL link may go down or link communications may be sporadic due to line errors and consequent retransmissions. The Switch does not automatically resume a dropped link if you use this mode.</p> <p><b>Dynamic rate adaptation:</b> the Switch dynamically changes the transmission rate negotiated between the Switch and CPE devices during initialization as well as during SHOWTIME status. This mode increases the line's stability and avoid the line being easily dropped when noise occurs. However, it may cause crosstalk noise during transmission rate adjustment.</p> <p><b>SOS enabled:</b> the Switch uses the emergency rate adjustment system for immediate rate adjustment to avoid crosstalk noise. See <a href="#">SOS on page 100</a> for more information.</p>
Retransmission Mode	<p>This field displays G.INP retransmission mode.</p> <p><b>n/a:</b> no CPE device is connected to this port.</p> <p><b>RTX in use:</b> G.INP retransmission is enabled on the Switch.</p> <p><b>Mode Forbidden:</b> G.INP retransmission is disabled on the Switch.</p> <p><b>CPE not support:</b> The connected CPE device does not support G.INP retransmission.</p>
G.INP Framing Type	<p>This field displays the DTU (Data Transfer Unit) framing type used when G.INP is enabled.</p> <p><b>0:</b> G.INP is disabled on the Switch.</p> <p><b>1:</b> The DTU doesn't contain an 8-bit CRC.</p> <p><b>2:</b> There is an additional 8-bit CRC inserted at the end of the DTU.</p> <p><b>3:</b> An 8-bit CRC is inserted as the first octet of the DTU.</p> <p><b>4:</b> An 8-bit CRC is inserted as the first byte of the DTU.</p>

**Table 7** Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
Actual INP against REIN	This field displays the actual impulse noise protection (INP) levels guaranteed on the latency path against REIN (Repetitive Electrical Impulse Noise) which is related to AC power frequency.
RS CW per DTU	This field displays the number of Reed-Solomon codewords per DTU (Data Transfer Unit).
VDSL Band Status	
The fields in this section display the status for upstream bands 0, 1, 2, 3, 4 ( <b>U0, U1, U2, U3, U4</b> ) and downstream bands 1, 2, 3, 4 ( <b>D1, D2, D3, D4</b> ).	
SNR margin	This field displays signal-to-noise ratio margin for each upstream and downstream bands. <b>NA</b> displays when the band is not used.
Signal Attenuation	This field displays the signal attenuation status for each upstream and downstream bands. <b>NA</b> displays when the band is not used.
Line Attenuation	This field displays the line attenuation status for each upstream and downstream bands. <b>NA</b> displays when the band is not used.
Transmit Power	This field displays the transmission power for each upstream and downstream bands. <b>NA</b> displays when the band is not used.
Receive Power	This field displays the receiving power for each upstream and downstream bands. <b>NA</b> displays when the band is not used.
VDSL Performance	
This section displays current VDSL performance measured from the Switch ( <b>Vtuc</b> ) and CPE side ( <b>Vtur</b> ) for the following three measurement durations.	
<ul style="list-style-type: none"> <li>• Since Link: This field displays the VDSL performance information recorded since the line was last up.</li> <li>• Curr 15 Min: This field displays the VDSL performance information recorded in the last 15 minutes.</li> <li>• Curr 1 Day: This field displays the VDSL performance information recorded in the past one day.</li> </ul>	
Full Inits	This field displays how many full initialization attempts on the line (successful and failed) there were.
Failed Full Inits	This field displays the number of failed full initialization attempts on the line.
FECS	This field displays the number of seconds at least one FEC (Forward Error Correction) event occurred on this line.
ES	This field displays the number of seconds the following events occurred on this line: <ul style="list-style-type: none"> <li>• The Switch: CRC-8, LOS, SEF or LPR value greater than or equal to 1 on the line.</li> <li>• CPE side: FEBE, LOS-FE, RDI or LPR-FE value greater than or equal to 1 on the line.</li> </ul>
SES	This field displays the number of seconds during this interval that: <ul style="list-style-type: none"> <li>• The Switch: LOS, SEF or LPR value was greater than or equal to 1 or the number of CRC-8 anomalies greater than or equal to 18 times on the line.</li> <li>• CPE side: LOS-FE, RDI or LPR-FE value was greater than or equal to 1 or the number of FEBE anomalies greater than or equal to 18 times on the line.</li> </ul>
LOSs	This field displays the count of 1-second intervals containing one or more Loss of Signal (LOS) failures.
LOFs	This field displays the count of 1-second intervals containing one or more Loss of Framing (LOF) failures.
UAS	This field displays the count of 1-second intervals for which the line is unavailable. Use this to define this line tolerance to allow how long for a period of Unavailable Seconds (UAS). Refer to ITU-T G997.1 chapter 7.2.1.1.5 for more detailed information.
Code Violation	This field displays the number of code words containing one or more anomalies.
Corrected	This field displays the number of code words containing one or more error blocks that have been corrected.

**Table 7** Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
Uncorrected	This field displays the number of code words containing one or more error blocks that can not be corrected.
Rtx	This field displays the number of RS (Reed-Solomon) codewords or DTUs (Data Transfer Units) retransmitted through PhyR or G.INP retransmissions.
RtxCorrected	This field displays the number of RS codewords or DTUs that have been corrected through PhyR or G.INP retransmissions.
RtxUncorrected	This field displays the number of RS codewords or DTUs that were not corrected successfully through PhyR or G.INP retransmissions.
LEFTRs	This field displays the number of seconds during which the Error Free Throughput went below the pre-configured threshold.
MinEFTR	This field displays the lowest value of the Error Free Throughput within the current interval.
ErrFreeBits	This field displays the number of bits that passed through the alpha1/beta1 interface (bits that are available to carry user payload).
LOLs/LOL	This field displays the count of 1-second intervals containing one or more Loss Of Link (LOL) failures and the number of times an LOL failure occurred.
LPRs/LPR	This field displays the count of 1-second intervals containing one or more PowerR (LPR) failures and the number of times an LPR failure occurred.
Time Elapsed	This field displays how many seconds has elapsed currently in this 15-minute (900 seconds) time segment. The counter restarts to zero after entering the next time segment.
VDSL Performance History	<p>Click the <b>15 Min Interval</b> link to display a screen listing VDSL performance information for the previous 15-minute periods.</p> <p>Click the <b>One Day Interval</b> link to display a screen listing VDSL performance information for the previous 24-hour periods.</p>
VDSL INM Performance History	<p>Click the <b>Current</b> link to display a screen listing INM (Impulse Noise Monitor) counters recorded since the link was last up or counters for the current 15-minute and 24-hour periods.</p> <p>Click the <b>15 Min Interval</b> link to display a screen listing INM counters for the previous 15-minute periods.</p> <p>Click the <b>One Day Interval</b> link to display a screen listing INM counters for the previous 24-hour periods.</p> <p>See <a href="#">Section 9.3.9 on page 119</a> on how to configure VDSL INM profiles which define INM control parameters.</p>
VDSL sub-carrier status	This section allows you to select the criteria below and display you the status in a raw data list or in a graph.
Items	<p>Select <b>Hlog</b> (Channel Transfer Function) to see the line's capability against interference and attenuation.</p> <p>Select <b>QLN</b> (Quiet Line Noise) to see the line's noise level.</p> <p>Select <b>SNR</b> (Signal-to-Noise-Ratio) to see the line's signal strength level.</p> <p>Select <b>BitAlloc</b> to display the number of bits allocated to each tone. The higher the bit allocated, the higher the data transmission rate.</p> <p>Select <b>GainAlloc</b> to display the gain allocated to each tone. Normally, each tone gets a different gain value allocated to avoid interference.</p>
Direction	Select <b>Downstream</b> or <b>Upstream</b> for the direction. Select <b>Both</b> for both downstream and upstream directions.

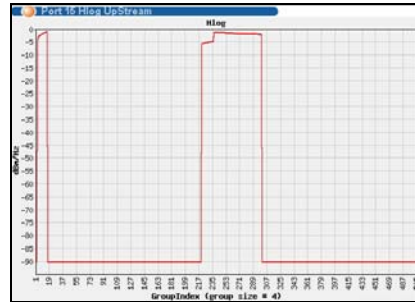
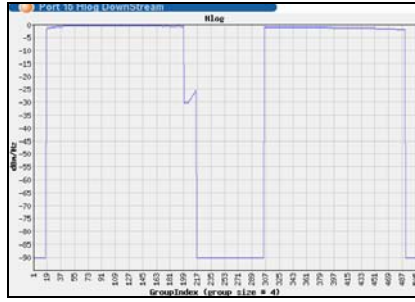
**Table 7** Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
Display	Select <b>Graph</b> or <b>Text</b> to display the graph or statistic data of the VDSL sub-carrier status. This field is not configurable and the Switch only displays the status in a graph when you select <b>Both</b> in the <b>Direction</b> field.
Show	Select the criteria above and click <b>Show</b> to display a screen where displays you port detail information in raw data or in a graph.
Measure	Click <b>Measure</b> to display the latest VDSL port details in this screen.
MEDLEY PSD	This section displays the final PSD the Switch proposes to the connected CPE during line initialization.
Break Point	This field displays the index number for each incremental break point.
Tone Index	This field displays the corresponding tone according to the specified break point.  A tone is a sub-channel of a VDSL band. DMT divides VDSL bands into many 4.3125 kHz tones.
PSD Level	This field displays the final PSD level the Switch proposes for the specified tone.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking <b>Set Interval</b> .
Stop	Click <b>Stop</b> to stop refreshing this screen.

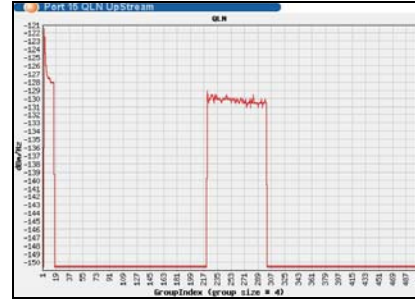
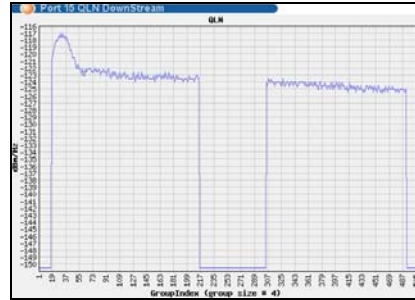
The following figures show you examples of each graph type that can be displayed when you click **Show** in the **VDSL sub-carrier status** section. Downstream information is in blue and upstream in red.

Figure 32 Graph Examples

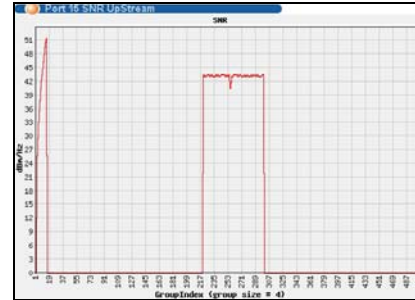
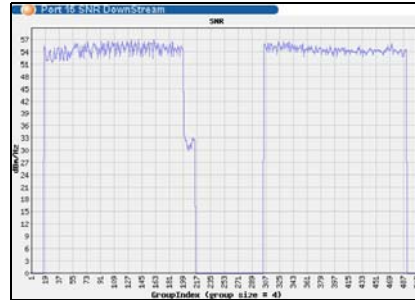
Hlog



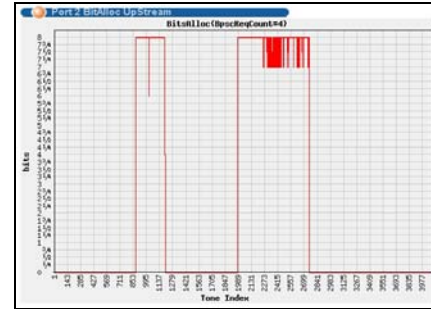
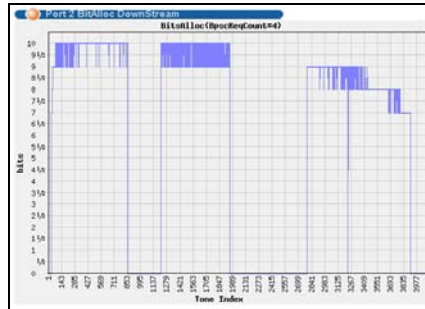
QLN



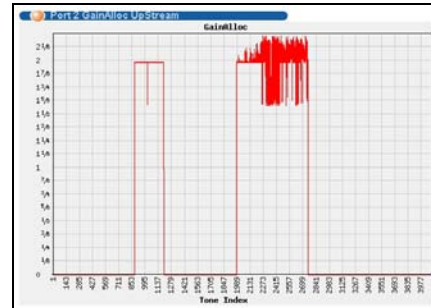
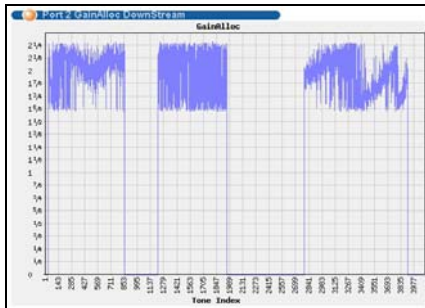
SNR



BitAlloc



GainAlloc





## 7.2.3 Bonding Group Details

Click a VDSL port's bonding group name in the **Group** column of the **Port Status** screen to display the following screen. Use this screen to check status for an individual VDSL bonding group on the Switch.

**Figure 33** Port Status: Bonding Group Details

Bonding Group Details		
Group Status	Group Name	B1
	Member Port	22,23
	Active Port	
	Main Port	22
	Transfer Mode	PTM
	Bonding Rate US	0.000Mbps
	Bonding Rate DS	0.000Mbps
Group Counter		
	Group Name	B1
	rxSmallFragments	0
	rxLargeFragments	0
	rxBadFragments	0
	rxLostFragments	0
	rxLostStarts	0
	rxLostEnds	0

The following table describes the labels in this screen.

**Table 8** Port Status: Bonding Group Details

LABEL	DESCRIPTION
Group Status	
Group Name	This shows the name of the VDSL port bonding group.
Member Port	This shows the ports in this bonding group.
Active Port	This shows the port(s) with connections up in this bonding group.
Main Port	This field displays the lower-numbered port in the VDSL port bonding group. This is the main port. The Switch records data sent and received counters based on this port.
Transfer Mode	This field displays the traffic type ( <b>PTM</b> or <b>ATM</b> ) of this bonding group.  Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard.  Asynchronous Transfer Mode (ATM) is a connection-oriented and cell-switching technology. It is supported by the ADSL/ADSL2/ADSL2+ standards.
Bonding Rate US	This field displays the current upstream rate for this bonding group.
Bonding Rate DS	This field displays the current downstream rate for this bonding group.
Group Counter	
Group Name	This shows the name of the VDSL port bonding group.
rxSmallFragments	The size of all data fragments should be the same and it is negotiated by the Switch and individual VDSL CPEs.  This shows the number of data fragments this group dropped due to being smaller than the negotiated size..

**Table 8** Port Status: Bonding Group Details (continued)

LABEL	DESCRIPTION
rxLargeFragments	This shows the number of data fragments this group dropped due to being bigger than the negotiated size.
rxBadFragments	This shows the number of data fragments this group received out of sequence.
rxLostFragments	This shows the number of missing data fragments that the Switch should have received.
rxLostStarts	This shows the number of beginning data fragments (with StartOfPacket indicator) that the Switch should have received but were lost.
rxLostEnds	This shows the number of ending data fragments (with EndOfPackets indicator) that the Switch should have received but were lost.

## 7.2.4 VDSL Summary

To view VDSL statistics, click **VDSL Summary** in the **Status** screen. Click **Clear** next to an entry to reset that connection. All values for that connection will be reset to 0.

**Figure 34** Status: VDSL Summary

Line NO	Name	State	Line Rate		Payload Rate		SNR Margin		Up/Down Statistics					Total Number of Packets	Clear		
			Up	Down	Up	Down	Up	Down	Total Number of Packets	Unicast Packets	Multicast Packets	Broadcast Packets	CRC Error Packets				
1		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
2	Showtime		19.890Mbps	80.326Mbps	19.819Mbps	80.071Mbps	26.8dB	25.7dB	1893	5	3	0	0	0	0	0	Clear
3		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
4		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
5		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
6		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
7		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
8		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
9		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
10		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
11		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
12		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
13		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
14		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
15		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
16		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
17		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
18		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
19		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear
20		Handshake	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Clear

## 7.2.5 Port Details

Click the **Port Details** link in the **VDSL Port Details** screen or an Ethernet port's index number in the **Port Status** screen to display the selected port's transmission statistics. Use this screen to check detailed transmission statistics for a selected VDSL port on the Switch.

**Figure 35** Port Details

Port Details		VDSL Port Details
<b>Port Info</b>	Port NO.	1
	Name	
	Link	Down
	Status	STOP
	LACP	Disabled
	TxPkts	0
	RxPkts	0
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	TxBytes	0
	RxBytes	0
	Bonding Up Time	---
	Up Time	0:00:00
<b>TX Packet</b>	<b>TX Packets</b>	0
	Multicast	0
	Broadcast	0
	Pause	0
	OutDiscards	0
	Tagged	0
	Drop	0
<b>RX Packet</b>	<b>RX Packets</b>	0
	Multicast	0
	Broadcast	0
	Pause	0
	InDiscards	0
	Control	0
	RateLimitDrop	0
	MeteringDrop	0
<b>TX Collision</b>	<b>Single</b>	0
	Multiple	0
	Excessive	0
	Late	0
<b>Error Packet</b>	<b>RX CRC</b>	0
	Runt	0
<b>Distribution</b>	<b>64</b>	0
	65 to 127	0
	128 to 255	0

The following table describes the labels in this screen.

**Table 9** Port Details

LABEL	DESCRIPTION
VDSL Port Details	Click this link to take you to a screen where you can view VDSL transmission statistics for the selected port.
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.

**Table 9** Port Details (continued)

LABEL	DESCRIPTION
Link	This field displays the speed (either <b>10M</b> for 10Mbps, <b>100M</b> for 100Mbps or <b>1000M</b> for 1000Mbps) and the duplex ( <b>F</b> for full duplex or <b>H</b> for half duplex). This field displays <b>Down</b> if the port is not connected to any device. This field also shows the cable type ( <b>Copper</b> or <b>Fiber</b> ).
Status	This field shows the training state of the ports. <b>FORWARDING</b> displayed if the link is functioning normally. Otherwise, it displays <b>STOP</b> .  When STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see <a href="#">Section 14.1 on page 160</a> for more information).
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxBkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Bonding Up Time	This field shows the total amount of time the port's link has been up.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet	
The following fields display detailed information about packets transmitted.	
TX Packets	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
OutDiscards	This field shows the number of outgoing packets discarded.
Tagged	This field shows the number of 802.1Q VLAN tagged packets transmitted.
RateLimitDrop	This field shows the number of outgoing packets dropped due to the guaranteed and/or maximum bandwidth limit are reached. You can configure the limit setting in the <b>Egress Rate</b> field of the <b>Basic Setting &gt; Rate Limit Profile Setup</b> screen.
Rx Packet	
The following fields display detailed information about packets received.	
RX Packets	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
InDiscards	This field shows the number of incoming packets discarded.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
RateLimitDrop	This field shows the number of incoming packets dropped due to the minimum bandwidth limit is reached. You can configure the limit setting in the <b>Ingress Commit Rate</b> and <b>Ingress Peak Rate</b> fields of the <b>Basic Setting &gt; Rate Limit Profile Setup</b> screen.
MeteringDrop	This field shows the number of the packets dropped due to the desired maximum bandwidth limit is reached. You can configure the limit setting in the <b>Management &gt; Policy Rule</b> screen. 0 displays if you did not configure the bandwidth limit in the associated policy or traffic amount is under the desired limit so far.

**Table 9** Port Details (continued)

LABEL	DESCRIPTION
TX Collision	
The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	
The following fields display detailed information about packets received that were in error.	
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65 to 127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128 to 255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256 to 511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512 to 1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024 to 1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	<p>This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size.</p> <p>The maximum frame size varies depending on your switch model. See <a href="#">Chapter 47 on page 381</a>.</p>

# Basic Setting

This chapter describes how to view and configure the Switch's basic settings for such as IP address, ports, hardware alarms.

## 8.1 Overview

The **System Info** screen displays general Switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general Switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your Switch. The real time is then displayed in the Switch logs. The **Switch Setup** screen allows you to set up and configure global Switch features. The **IP Setup** screen allows you to configure a Switch IP address in each routing domain, subnet mask(s) and DNS (domain name server) for management purposes. The **Port Setup** screen allows you to enable or disable a port on the Switch and configure the port settings, such as the speed and duplex mode.

## 8.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. You can check the firmware version number and monitor the Switch temperature, fan speeds and voltage in this screen. Note that the fan speed information in the **Hardware Monitor** table is not available for this model.

Figure 36 Basic Setting &gt; System Info

System Info	
System Name	VES1724-56
ZyNOS F/W Version	V56_Fanless130626   06/26/2013
Modem Code F/W Version	10.08.39
Ethernet Address	cc:5d:4e:00:00:02
Power Module	AC
1st F/W Version	V56_Fanless130626   06/26/2013
2nd F/W Version	V1015GPIO3   10/15/2012

Hardware Monitor					
Temperature Unit	<input type="button" value="C"/>				
Temperature (C)	Current	MAX	MIN	Threshold	Status
CPU	35.0	35.0	30.0	95.0	Normal
DSP#1	36.0	36.0	32.0	95.0	Normal
ADT7463	36.0	36.0	31.0	95.0	Normal
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
Voltage (V)	Current	MAX	MIN	Threshold	Status
14VIN	14.269	14.269	14.269	+/-10%	Normal
2.5VS	2.553	2.553	2.535	+/-5%	Normal
CPU/DSP/AFE	1.189	1.201	1.189	+/-5%	Normal

The following table describes the labels in this screen.

Table 10 Basic Setting &gt; System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Modem Code F/W Version	This field displays the version number of the VDSL chip firmware used in the Switch.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
Power Module	This field displays <b>Dual</b> when the Switch supports both AC and DC power input. Otherwise, it displays <b>AC</b> or <b>DC</b> when the corresponding power module is connected and detected.
1st F/W Version	This field displays the version number of the currently installed firmware on the first flash memory.
2nd F/W Version	This field displays the version number of the currently installed firmware on the second flash memory.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	<b>BOARD, MAC</b> and <b>PHY</b> refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays <b>Normal</b> for temperatures below the threshold and <b>Error</b> for those above.

**Table 10** Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure.
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	<b>Normal</b> indicates that this fan is functioning above the minimum speed. <b>Error</b> indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	<b>Normal</b> indicates that the voltage is within an acceptable operating range at this point; otherwise <b>Error</b> is displayed.

### 8.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting > General Setup** in the navigation panel to display the screen as shown.

**Figure 37** Basic Setting > General Setup



The following table describes the labels in this screen.

**Table 11** Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	<p>Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format.</p> <p>When you select the <b>Daytime (RFC 867)</b> format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone.</p> <p><b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p><b>NTP (RFC-1305)</b> is similar to Time (RFC-868).</p> <p><b>None</b> is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 1970-1-1 0:0.</p>
Time Server IP Address	Enter the IPv4 or IPv6 address of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format. The new time then appears in the <b>Current Time</b> field after you click <b>Apply</b> .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the <b>Current Date</b> field after you click <b>Apply</b> .
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Saving Time</b>. The time is displayed in the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Second, Sunday, March</b> and <b>2:00</b>.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b> and the last field depends on your time zone. In Germany for instance, you would select <b>2:00</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

**Table 11** Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Saving Time</b>. The time field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, November</b> and <b>2:00</b>.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b> and the last field depends on your time zone. In Germany for instance, you would select <b>2:00</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note: VLAN is unidirectional; it only governs outgoing traffic.

See [Chapter 10 on page 129](#) for information on port-based and 802.1Q tagged VLANs.

## 8.5 Switch Setup Screen

Click **Basic Setting** > **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLAN.

**Figure 38** Basic Setting > Switch Setup

The following table describes the labels in this screen.

**Table 12** Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose <b>802.1Q</b> or <b>Port Based</b> . The <b>VLAN Setup</b> screen changes depending on whether you choose <b>802.1Q</b> VLAN type or <b>Port Based</b> VLAN type in this screen. See <a href="#">Chapter 10 on page 129</a> for more information.
Bridge Control Protocol Transparency	Select <b>Active</b> to allow the Switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the <b>Port Setup</b> screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be released).
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a <b>Join</b> message using GARP. Declarations are withdrawn by issuing a <b>Leave</b> message. A <b>Leave All</b> message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a <b>Join Period</b> timer. The allowed <b>Join Time</b> range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.

**Table 12** Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
Leave Timer	Leave Time sets the duration of the <b>Leave Period</b> timer for GVRP in milliseconds. Each port has a single <b>Leave Period</b> timer. Leave Time must be two times larger than <b>Join Timer</b> ; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment	
IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next fields to configure the priority level-to-physical queue mapping.	
The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields.

## 8.6 IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to  $3.4 \times 10^{38}$  IP addresses.

### 8.6.1 IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0.

- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.

## 8.6.2 IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (2001:db8) is the subnet prefix.

## 8.6.3 IPv6 Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

The first 48 bits of the IPv6 subnet mask are for Internet routing or fixed for local address, the 49th to the 54th bits are for subnetting and the last 64 bits are for interface identifying. The 16 binary digits for subnetting allows an organization to set up to 65,535 individual subnets.

## 8.6.4 Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

## 8.6.5 Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

**Table 13** Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

## 8.6.6 Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3. The global address format as follows.

**Table 14** Global Address Format

001	Global ID	Subnet ID	Interface ID
3 bits	45 bits	16 bits	64 bits

The global ID is the network identifier or prefix of the address and is used for routing. This may be assigned by service providers.

The subnet ID is a number that identifies the subnet of a site.

## 8.6.7 Unspecified

An unspecified address (0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

## 8.6.8 EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits ffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC            00 : 13 : 49 : 12 : 34 : 56

EUI-64        02 : 13 : 49 : FF : FE : 12 : 34 : 56

## 8.6.9 Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see [Interface ID](#) and [EUI-64](#)) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the `ipv6 address autoconfig` command is issued on the Switch, it generates <sup>1</sup>another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

1. In IPv6, all network interfaces can be associated with several addresses.

## 8.7 IP Setup

Use the **IP Setup** screen to configure the Switch IP address, default gateway device, the default domain name server and the management VLAN ID. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

### 8.7.1 Management IP Addresses

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

You can configure up to 64 IP addresses which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s).

Note: You must configure a VLAN first.

**Figure 39** Basic Setting > IP Setup

**IP Setup**

Domain Name Server: 0.0.0.0

Default Management:  In-band  Out-of-band

**In-band Management IP Address**

DHCP Client

DHCP Option 12: DSLAM VES1724-...

DHCP Option 60: DSLAM cc5d-4e00

Static IP Address

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

VID: 1

**Out-of-band Management IP**

IP Address: 192.168.0.1

Apply Cancel

**In-band IP Addresses (VPS)**

IP Address (VPS)	IP Subnet Mask	VID	Default Gateway	Manageable	Delete
0.0.0.0	0.0.0.0		0.0.0.0	<input type="checkbox"/>	

Add Cancel

Index	IP Address (VPS)	IP Subnet Mask	VID	Default Gateway	Manageable	Delete

Delete Cancel

The following table describes the labels in this screen.

**Table 15** Basic Setting > IP Setup

LABEL	DESCRIPTION
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow ( <b>In-Band</b> or <b>Out-of-band</b> ) the Switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source.  Select <b>Out-of-band</b> to have the Switch send the packets to the out-of-band management port. This means that device(s) connected to the other port(s) do not receive these packets.  Select <b>In-Band</b> to have the Switch send the packets to all ports except the out-of-band management port to which connected device(s) do not receive these packets.
In-Band Management IP Address	
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
DHCP Option 12	Select this and specify the Switch's name in the text box to have the Switch add the information into the DHCP request messages the Switch sends.
DHCP Option 60	Select this and specify the Switch's vendor type to have the Switch add the information into the DHCP request messages the Switch sends.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
VID	Enter the VLAN identification number associated with the Switch IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the Switch make sure the port that you are connected to is a member of Management VLAN.
Out-of-band Management IP Address	
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.0.1.  If you change this IP address, make sure the computer connected to this management port is in the same subnet before accessing the Switch.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.0.254.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring the fields again.



**Table 15** Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
In-band IP Addresses (VPS)	
You can create up to 64 IPv4 addresses, which are used to access and manage the Switch from the ports belonging to the pre-defined VLANs. You must configure a VLAN first. VPS stands for Virtual Private Server which virtually divides a device into several servers, each handling its own traffic independently.	
IP Address (VPS)	Enter the IP address for managing the Switch by the members of the VLAN specified in the <b>VID</b> field below.
IP Subnet Mask	Enter the IP subnet mask in dotted decimal notation.
VID	Type the VLAN group identification number.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.
Manageable	Select this to allow the Switch to be managed by connections to this specified IP address in the specified VLAN.
Add	Click <b>Add</b> to insert the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
IP Address (VPS)	This field displays the IP address.
IP Subnet Mask	This field displays the subnet mask.
VID	This field displays the ID number of the VLAN group.
Default Gateway	This field displays the IP address of the default gateway.
Manageable	This field displays whether the Switch can be managed using this specified IP address.
Delete	Check the management IP addresses that you want to remove in the <b>Delete</b> column, then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected check boxes in the <b>Delete</b> column.

## 8.8 External Alarm Switch

Use this screen to view the status of the external alarm inputs and configure their settings.

**Figure 40** Basic Setting > External Alarm Switch

Index	Status	Enable	Name
1	Normal	<input checked="" type="checkbox"/>	<input type="text"/>
2	Normal	<input checked="" type="checkbox"/>	<input type="text"/>
3	Normal	<input checked="" type="checkbox"/>	<input type="text"/>
4	Normal	<input checked="" type="checkbox"/>	<input type="text"/>

The following table describes the labels in this screen.

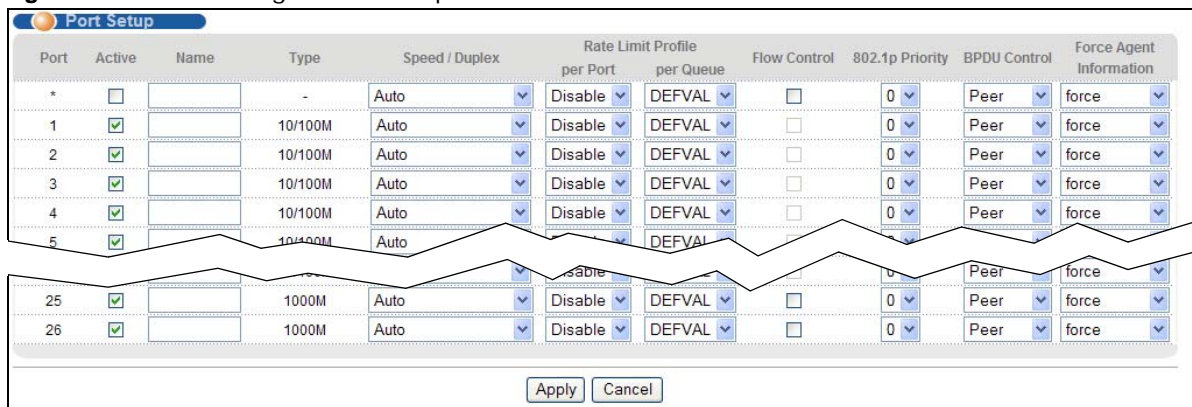
**Table 16** Basic Setting > External Alarm Switch

LABEL	DESCRIPTION
Index	This is the index number of the external alarm input.
Status	This field displays whether the external alarm input has alarms ( <b>Alarm</b> ) or not ( <b>Normal</b> ). <b>Disable</b> displays if the external alarm input is not in use.
Enable	Select this check box to have the Switch use the external alarm input.
Name	Enter a descriptive name that identifies this alarm input. You can enter up to 31 printable characters. Spaces are also allowed.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.9 Port Setup

Use this screen to configure Switch port settings. Click **Basic Setting > Port Setup** in the navigation panel to display the configuration screen.

**Figure 41** Basic Setting > Port Setup



The following table describes the labels in this screen.

**Table 17** Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.

**Table 17** Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Name	<p>Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters.</p> <p>Note: Due to space limitation, the port name may be truncated in some Web Configurator screens.</p>
Type	<p>This field displays <b>10/100M</b> for Fast Ethernet connections and <b>10/100/1000M</b> for Gigabit connections.</p>
Speed/Duplex	<p>Select the speed and the duplex mode of the Ethernet connection on this port. Choices are <b>Auto</b>, <b>10M/Half Duplex</b>, <b>10M/Full Duplex</b>, <b>100M/Half Duplex</b>, <b>100M/Full Duplex</b> and <b>1000M/Full Duplex</b> (Gigabit connections only).</p> <p>Selecting <b>Auto</b> (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p>
Rate Limit Profile	<p>These fields display the rate limit profile names you configure in the <b>Rate Limit Profile Setup</b> screens. Refer to <a href="#">Section 8.10 on page 84</a> for more information.</p>
per Port	<p>Select a rate limit profile from the drop-down list box. You can define the maximum incoming and outgoing transmission data rate on a per-port basis.</p>
per Queue	<p>Select a per queue rate limit profile from the drop-down list box. You can define the maximum incoming and outgoing transmission data rate on a per-queue basis.</p>
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. <b>Flow Control</b> is used to regulate transmission of signals to match the bandwidth of the receiving port.</p> <p>The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select <b>Flow Control</b> to enable it. This field is available for an Ethernet port only.</p>
802.1p Priority	<p>This priority value is added to incoming frames without a (802.1p) priority queue tag. See <b>Priority Queue Assignment</b> in <a href="#">Table 12 on page 75</a> for more information.</p>

**Table 17** Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
BPDU Control	<p>Configure the way to treat BPDUs (Bridge Protocol Data Units) received on this port. You must activate bridging control protocol transparency in the <b>Switch Setup</b> screen first.</p> <p>Select <b>Peer</b> to look at the information in the received BPDUs. For example, the root bridge's existence, if any bridge was added or removed from the STP (Spanning Tree Protocol) network, if any loop occurred in the STP network.</p> <p>Select <b>Tunnel</b> to add the incoming port's PVID on the received BPDUs and then forward them to the next Switch.</p> <p>Select <b>Discard</b> to drop all BPDUs received on this port. Set this only on an edge port of a STP network.</p> <p>Select <b>Network</b> to forward VLAN-tagged BPDUs to the next Switch directly and handle VLAN-untagged BPDUs as the <b>Peer</b> option.</p> <p>See <a href="#">Section 14.1.2 on page 161</a> for more information about BPDUs.</p>
Force Agent Information	<p>Select <b>force</b> to allow the Switch to add/replace a DHCP option 82 tag in the corresponding packets received by this port for the following applications:</p> <ul style="list-style-type: none"> <li>• PPPoE IA (See <a href="#">Section 32.4 on page 291</a> and <a href="#">Section 32.5 on page 293</a>)</li> <li>• DHCP relay (See <a href="#">Section 35.4.4 on page 314</a>)</li> <li>• DHCP VLAN (See <a href="#">Section 35.5 on page 318</a>)</li> <li>• DHCP snooping (See <a href="#">Section 26.5.2 on page 260</a>)</li> </ul> <p>Select <b>transparent</b> to ignore the PPPoE IA and DHCP option 82 tag settings of packets received on this port.</p>
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.10 Rate Limit Profile Setup

Rate limit profiles define ingress and egress data rate limits for the Switch port(s).

Click **Basic Setting** and **Rate Limit Profile Setup** in the navigation panel to display the screen as shown.

**Figure 42** Rate Limit Profile Setup

**Rate Limit Profile Setup** Per Queue

Name

Ingress Commit Rate(Kbps)   (minimum scale is 64Kbps)

Ingress Peak Rate(Kbps)   (minimum scale is 64Kbps)

Egress Rate(Kbps)   (minimum scale is 64Kbps)

Name	Ingress Commit	Ingress Peak	Egress	Applied Ports	Delete
Disable	-	-	-	1-26	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 18** Rate Limit Profile Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 20 characters) for identification purposes.
Ingress Commit Rate(Kbps)	Select the checkbox and enter the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow through a port. Enter a number between 64 and 1000000. Alternatively, clear the checkbox to not use the rate limit.  Note: The sum of commit rate cannot be greater than or equal to the uplink bandwidth.
Ingress Peak Rate(Kbps)	Select the checkbox and enter the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow through a port when burst traffic occurs. The incoming traffic over this peak rate will be discarded. Enter a number between 64 and 1000000. Alternatively, clear the checkbox to not use the rate limit.  Note: The peak rate should be greater than the commit rate.
Egress Rate(Kbps)	Select the checkbox and enter the maximum bandwidth allowed in kilobits per second (Kbps) for the outgoing traffic flow through a port. Enter a number between 64 and 1000000. Alternatively, clear the checkbox to not use the rate limit.
Add	Click <b>Add</b> to save the new rule to the switch. Then a summary table displays in the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name for the rate limit profile.
Ingress Commit	This field displays the ingress committed rate limit for the port(s)
Ingress Peak	This field displays the ingress peak rate limit for the port(s)
Egress	This field displays the egress rate limit for the port(s).
Applied Ports	This field displays the port number(s) to which this profile is applied.  You can apply a rate limit profile to a port in the <b>Port Setup</b> screen.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

### 8.10.1 Per Queue Ratelimit Profile

You can also use per queue rate limit profiles to define ingress and egress data rate limits for each queue on the Switch.

Click the **Per Queue** link in the **Rate Limit Profile Setup** screen to display the screen as shown.

**Figure 43** Rate Limit Profile Setup > Per Queue

The screenshot shows the 'Per Queue Rate Limit Profile' configuration interface. At the top, there is a title bar with an orange icon and the text 'Per Queue Rate Limit Profile'. Below this is a 'Name' input field. The main area contains a table with three columns: 'Queue' (index 0-7), 'CIR (64 Kbps granularity)', and 'PIR (64 Kbps granularity)'. Each row has a corresponding input field. Below the table are 'Add' and 'Clear' buttons. At the bottom, there is a summary table with four columns: 'Index', 'Name', 'Applied Ports', and 'Delete'. The first row in the summary table shows '1', 'DEFVAL', '1-26', and a checkbox.

The following table describes the labels in this screen.

**Table 19** Rate Limit Profile Setup > Per Queue

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 20 characters) for identification purposes.
Queue	This is the index number of queues on the Switch. The Switch has eight physical queues.
CIR	Select the checkbox and enter the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow assigned to this queue through a port. Enter a number between 64 and 1000000. The sum of commit rate cannot be greater than or equal to the uplink bandwidth.
PIR	Select the checkbox and enter the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow assigned to this queue through a port when burst traffic occurs. The incoming traffic over this peak rate will be discarded. Enter a number between 64 and 1000000. The peak rate should be greater than the commit rate.
Add	Click <b>Add</b> to save the new rule to the Switch. Then a summary table displays in the bottom of the screen.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to edit the profile.
Name	This field displays the descriptive name for the profile.
Applied Ports	This field displays the port number(s) to which this profile is applied. You can apply a rate limit profile to a port in the <b>Port Setup</b> screen.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 8.11 Hardware Alarm Profile

Click **Basic Setting** > **Hardware Alarm Profile** to display the screen as shown. Hardware alarm profile defines CPU, packet buffer, memory utilization thresholds and CPU, DSP, ADT temperature thresholds. The Switch sends a hardware alarm once it detects one usage over its pre-defined threshold. Configure the thresholds and click **Apply** to save your changes or click **Cancel** to reload the previous settings for this screen.

**Figure 44** Hardware Alarm Profile Setup

Utilization Threshold		
CPU Utilization	0	%
Packet Buffer	0	%
Memory Usage	0	%

Temperature High Threshold		
CPU	95	°C
DSP	95	°C
ADT	95	°C

Apply Cancel

## 8.12 CPE Port Status

Use this screen to view all DSL port status and details about the connected CPE devices.

**Figure 45** CPE Port Status

Port	Link State	Actual NDR US/DS(Mbps)	Model	Modem Code	FW Version	Wireless	VDSL Template	Line Profile	Channel Profile	Inm Profile
1	Handshake	0.000 / 0.000	N/A	N/A	N/A	N/A	DEFVAL	DEFVAL	DEFVAL	DEFVAL
2	Handshake	0.000 / 0.000	N/A	N/A	N/A	N/A	DEFVAL	DEFVAL	DEFVAL	DEFVAL
3	Handshake	0.000 / 0.000	N/A	N/A	N/A	N/A	DEFVAL	DEFVAL	DEFVAL	DEFVAL
22- B01*	Handshake	0.000 / 0.000	N/A	N/A	N/A	N/A	DEFVAL	DEFVAL	DEFVAL	DEFVAL
23- B01	Handshake	0.000 / 0.000	N/A	N/A	N/A	N/A	DEFVAL	DEFVAL	DEFVAL	DEFVAL
24	Handshake	0.000 / 0.000	N/A	N/A	N/A	N/A	DEFVAL	DEFVAL	DEFVAL	DEFVAL

The following table describes the labels in this screen.

**Table 20** Basic Setting > CPE Port Status

LABEL	DESCRIPTION
Port	This is the number of a port.
Link State	This field displays <b>Showtime</b> when the DSL connection is up. Otherwise, it displays <b>Idle</b> , <b>Handshake</b> or <b>Training</b> during the DSL line establishment. If you perform a DELT test, this field will display <b>LD_Testing</b> . The state changes to <b>LD_Done</b> after the DELT test is completed.
Actual NDR US/DS(Mbps)	This field displays the actual upstream/downstream net data rate in Mbps.
Model	This field displays the model name of the CPE device connected to this port. <b>NA</b> displays if it is not available.

**Table 20** Basic Setting > CPE Port Status (continued)

LABEL	DESCRIPTION
Modem Code	This field displays the chip firmware version number of the CPE device connected to this port. <b>NA</b> displays if it is not available.
FW Version	This field displays the firmware version number of the DSL CPE device connected to this port. <b>NA</b> displays if it is not available.
Wireless	This field displays whether or not the CPE device has the wireless function enabled. <b>NA</b> displays if it is not available.
VDSL Template	This field displays the name of the VDSL profile applied to this DSL connection.
Line Profile	This field displays the name of the line profile applied to this DSL connection.
Channel Profile	This field displays the name of the channel profile applied to this DSL connection.
Inm Profile	This field displays the name of the INM profile applied to this DSL connection.

## 8.13 IPv6 Setup

Use this screen to configure Switch's management IPv6 addresses. Click **Basic Setting > IP Setup > IPv6 Setup** to display the configuration screen. See [Section 8.6 on page 76](#) for more information about IPv6.

**Figure 46** Basic Setting > IPv6 Setup

**IPv6** [IPv6 Neighbor Setup](#)

**IPv6 Default Management Setup**

IPv6 Interface: NONE

Apply Cancel

**IPv6 Interface Setup**

IPv6 Group:  Inband  Outband

VID:

IPv6:  Enable  Disable

Default Gateway:

Enable IPv6 autoconfig:

Add Cancel

Index	Interface	IPv6 Status	Default Gateway	AutoConfig	Configuration	Delete
1	<a href="#">VLAN1</a>	Enable	::	Yes	<a href="#">Click Here</a>	<input type="checkbox"/>

Delete Cancel



The following table describes the labels in this screen.

**Table 21** Basic Setting > IPv6 Setup

LABEL	DESCRIPTION
IPv6 Default Management Setup	
IPv6 Interface	Select an in-band interface (VLAN1 ~ VLAN4094) or an out-of-band interface ( <b>MGMT0</b> ) to forward IPv6 packets for which the Switch cannot find a specific interface to route. Select <b>NONE</b> to not specify the default IPv6 interface.  You have to first configure an IPv6 interface in the <b>IPv6 Interface Setup</b> section below before setting it as the default interface here.
Apply	Click <b>Apply</b> to save your change to the Switch's run-time memory. The Switch loses the change if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
IPv6 Interface Setup	
IPv6 Group	Select to configure IPv6 settings for the in-band or the out-of-band IPv6 interface.
VID	This field is available when you select <b>Inband</b> in the <b>IPv6 Group</b> field above.  Enter the VLAN identification number associated with the Switch's IPv6 address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the Switch from any port. If a port is not a member of this VLAN, then users on that port cannot manage the Switch. To access the Switch make sure the port that you are connected to is a member of the management VLAN.
IPv6	Enable or disable IPv6 for this interface.
Default Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Enable IPv6 autoconfig	Select <b>Enable</b> to allow the IPv6 hosts connected to this interface to automatically generate unique IPv6 addresses by combining the network prefix advertised from the router and their interface IDs.
Add	Click <b>Add</b> to save the new settings to the Switch. They then display in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Index	This is the index number of the entry.
Interface	This is the name of the interface. Click the link to view the details.
IPv6 Status	This displays whether IPv6 is enabled or not on this interface.
Default Gateway	This displays the IPv6 address of the default gateway.
AutoConfig	This displays whether IPv6 stateless autoconfiguration is enabled or not. <b>Yes</b> displays if this interface allows the connected IPv6 hosts to automatically generate unique IPv6 addresses by combining the network prefix advertised from the router and their interface IDs. Otherwise, this field displays <b>No</b> .
Configuration	Click the <b>Click Here</b> link to configure additional IPv6 settings for this interface.
Delete	Select entries to remove in the <b>Delete</b> column and then click the <b>Delete</b> button to remove them.
Cancel	Click <b>Cancel</b> to clear the selected checkbox(es) in the <b>Delete</b> column.

### 8.13.1 IPv6 Setup: Configuration

Click the **Click Here** link in the **Configuration** field at the bottom of the **Basic Setting > IPv6 Setup** screen to display the configuration screen. Use this screen to view and configure static IPv6 addresses for the interface.

**Figure 47** Basic Setting > IPv6 Setup > Configuration: Click Here

The screenshot shows the IPv6 Setup Configuration screen. At the top, there are tabs for 'IPv6 Setup' and 'IPv6 ND Setup'. Below the tabs, the 'Static IPv6 Addresses' section contains a form with the following fields:

- Interface Name: MGMT0
- IPv6 Address: [text input field]
- IPv6 Prefix Length: [text input field]
- EUI-64 format:

Below the form are 'Add' and 'Cancel' buttons. At the bottom of the screen, there is a table with the following data:

Index	Interface	IPv6 Address / Prefix Length	Delete
<a href="#">1</a>	MGMT0	2001::ce5d:4eff:fe00:1/64	<input type="checkbox"/>

Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 22** Basic Setting > IPv6 Setup > Configuration: Click Here

LABEL	DESCRIPTION
Interface Name	This field displays the name of the IPv6 interface.
IPv6 Address	Enter an IPv6 address for this interface. An IPv6 interface can have multiple IPv6 addresses.
IPv6 Prefix Length	Enter the IPv6 prefix length (1~128) for this interface. For a link-local IPv6 address, enter 64 here.
EUI-64 format	If you are configuring an IPv6 global address, select this to use the EUI-64 format to generate an interface ID from the MAC address of the interface. See <a href="#">Section 8.6.8 on page 78</a> for more information.
Add	Click <b>Add</b> to save the new settings to the Switch. The setting displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Index	This field displays the index number of an entry. Click the link to display the settings in the <b>Static IPv6 Addresses</b> section above so you can view and modify the settings.
Delete	Select entries to remove in the <b>Delete</b> column and then click the <b>Delete</b> button to remove them.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 8.13.2 IPv6 ND Setup

Click the **IPv6 ND Setup** link in the **Basic Setting > IPv6 Setup > Configuration: Click Here** screen to display the configuration screen. Use this screen to view and configure the neighbor discover settings for the interface.

**Figure 48** Basic Setting > IPv6 Setup > Configuration: Click Here > IPv6 ND Setup

Neighbor Discover Setup	
Interface	MGMT0
DAD Attempts	1
NS Interval(ms)	1000
Reachable Time(ms)	30000

The following table describes the labels in this screen.

**Table 23** Basic Setting > IPv6 Setup > Configuration: Click Here > IPv6 ND Setup

LABEL	DESCRIPTION
Interface	This field displays the name of the IPv6 interface.
DAD Attempts	Enter the number of DAD (Duplicate Address Detection) messages the Switch can send for checking whether an IPv6 address is available before assigning it to the interface. Possible values are 1-7. Enter 0 here to have the Switch not send any DAD messages.
NS Interval(ms)	Enter the time in milliseconds between neighbor solicitation packet retransmissions. Possible values are 1000-4294967295.
Reachable Time(ms)	Enter the time in milliseconds that can elapse before a neighbor is detected. Possible values for this field are 0-3600000.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.13.3 IPv6 Neighbor Setup

Use this screen to configure a static entry in the IPv6 neighbor discovery cache, which lists the MAC addresses of the Switch's interfaces and neighboring devices. This cache table is similar to a MAC address table in IPv4. You can only configure static entries on an IPv6-enabled interface.

Click the **IPv6 Neighbor Setup** link in the **Basic Setting > IPv6 Setup** screen to display the configuration screen.

**Figure 49** Basic Setting > IPv6 Setup > IPv6 Neighbor Setup

The following table describes the labels in this screen.

**Table 24** Basic Setting > IPv6 Setup > IPv6 Neighbor Setup

LABEL	DESCRIPTION
Static Neighbor Cache Setting	
IPv6 Group	Select whether the Switch uses the inband or the outband interface to reach the neighbor device.
VID	This field is available when you select <b>Inband</b> in the <b>IPv6 Group</b> field above. Enter the VLAN ID (1~4094) associated with the specified IPv6 address below.
IPv6 Address	Enter an IPv6 address for a static neighbor entry.
MAC Address	Enter the MAC address for the static neighbor entry.
Add	Click <b>Add</b> to save the new settings to the Switch. The setting displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Index	This field displays the index number of a neighbor entry.
Interface	This field displays the name of the interface the Switch uses to reach the neighboring interface.
IPv6 Address	This field displays the IPv6 address of the neighboring interface.
MAC Address	This field displays the MAC address of the neighboring interface.

**Table 24** Basic Setting > IPv6 Setup > IPv6 Neighbor Setup (continued)

LABEL	DESCRIPTION
State	<p>This field displays whether the neighboring IPv6 interface is reachable. In IPv6, "reachable" means an IPv6 packet can be correctly forwarded to a neighboring node (host or router) and the neighbor can successfully receive and handle the packet. This field can display:</p> <p><b>Reachable:</b> The interface of the neighboring device is reachable. (The Switch has received a response to its neighbor solicitation.)</p> <p><b>Stale:</b> The last reachable time has expired or the Switch received an unrequested advertisement that updates the cached link-layer address from the neighboring interface.</p> <p><b>Delay:</b> A packet is being sent to the neighboring interface in <b>Stale</b> state. The Switch delays sending request packets for a short time to give upper-layer protocols a chance to determine reachability. If no reachability confirmation is received within the delay timer, the Switch sends a neighbor solicitation and changes the state to <b>Probe</b>.</p> <p><b>Probe:</b> The Switch is sending neighbor solicitations and waiting for the neighbor's response.</p> <p><b>Invalid:</b> The neighbor address is an invalid IPv6 address.</p> <p><b>Unknown:</b> The status of the neighboring interface can not be determined.</p> <p><b>Incomplete:</b> Address resolution is in progress and the link-layer address of the neighbor has not yet been determined (see RFC 4861). The interface of the neighboring device did not give a complete response.</p>
Link Type	<p>This field displays the type of the IPv6 address.</p> <p><b>Local:</b> The IPv6 address belongs to an interface on the Switch.</p> <p><b>Static:</b> The IPv6 address belongs to a neighboring interface and it has been configured manually on the Switch.</p> <p><b>Dynamic:</b> The IPv6 address belongs to a neighboring interface and the Switch has learned it dynamically.</p> <p><b>Other:</b> The IPv6 address belongs to none of the types above.</p>
Delete	<p>Select entries to remove in the <b>Delete</b> column and then click the <b>Delete</b> button to remove them.</p>
Cancel	<p>Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.</p>

## 8.14 SFP Threshold Setup

Use this screen to view the status of the Small Form-factor Pluggable (SFP) mini-GBIC transceivers installed in the Switch's SFP slots. You can also set thresholds for sending traps based on the SFP module's operating parameters such as transceiver temperature, laser bias current, transmitted optical power, received optical power and transceiver supply voltage. **N/A** displays if the Switch does not detect a mini-GBIC transceiver in an SFP slot.

Click **Basic Setting** > **SFP Threshold Setup** in the navigation panel to display the screen as shown.

**Figure 50** Basic Setting > SFP Threshold Setup

The following table describes the labels in this screen.

**Table 25** Basic Setting > SFP Threshold Setup

LABEL	DESCRIPTION
User Input Enable	Select this option if you want to apply the threshold settings configured at the bottom of the screen.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Port Index	Select an SFP slot of the Switch for which you want to configure the thresholds.
Type	This is the type of device operating parameters.
Current	This shows the current value of each parameter measured for the installed transceiver.

**Table 25** Basic Setting > SFP Threshold Setup (continued)

LABEL	DESCRIPTION
High Alarm Threshold	Specify the first upper limit for each parameter. The Switch sends an alarm trap when one of the parameter values goes over this value.
High Warning Threshold	Specify the second upper limit for each parameter. The Switch sends a warning trap when one of the parameter values goes over this value. This value should be smaller than the <b>High Alarm Threshold</b> and greater than the <b>Low Warning Threshold</b> .
Low Warning Threshold	Specify the first lower limit for each parameter. The Switch sends a warning trap when one of the parameter values falls below this value. This value should be smaller than the <b>High Warning Threshold</b> and greater than the <b>Low Alarm Threshold</b> .
Low Alarm Threshold	Specify the second lower limit for each parameter. The Switch sends an alarm trap when one of the parameter values falls below this value. This value should be smaller than the <b>Low Warning Threshold</b> .
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
SFP Transceiver Per Port Status	
Port	This field displays the port number of the SFP slots.
Vendor	This field displays the vendor of the transceiver installed in the slot.
Part Number	This field displays the part number defined by the transceiver vendor.
Series Number	This field displays the serial number of the transceiver.
Revision	This field displays the version of the transceiver.
Transceiver	This field displays the name of the transceiver.
Current Temperature(C)	This field displays the current temperature inside the SFP module.
Voltage(V)	This field displays the level of voltage currently being supplied to the SFP module.
Tx Bias(mA)	This field displays the current in milliamps (mA) being supplied to the SFP module's Laser Diode Transmitter. Track the Tx bias to know how the laser component is aging relative to your network's other SFP modules. This helps you know when to do preventative maintenance instead of having to deal with an unexpected SFP module failure.
Tx Power(dBm)	This field displays the amount of light (in dBm) the SFP module is currently transmitting. This value does not reflect the condition of the cable. Refer to this number to monitor the laser's health.
Rx Power(dBm)	This field displays the amount of light (in dBm) currently being received from the fiber optic cable.





# VDSL Setup

## 9.1 VDSL Overview

Very High Bit Rate DSL is an asymmetric version of DSL that is used as the final drop from a fiber optic junction point to nearby customers. VDSL lets an apartment or office complex obtain high-bandwidth services using existing copper wires without having to replace the infrastructure with optical fiber. Like ADSL, VDSL can share the line with the telephone.

Your Switch supports VDSL2 (Very High Speed Digital Subscriber Line 2) which is the second generation of the VDSL standard (which is currently denoted VDSL1). VDSL2 allows a frequency band of up to 30MHz and transmission rates of up to 100 Mbps in each direction. VDSL2 is defined in G.993.2.

### VDSL Parameters

The following sections describe the VDSL parameters you configure in the following screens:

- [VDSL Template Setup](#) (see [Section 9.3 on page 104](#)).
- [VDSL Alarm Template Setup](#) (see [Section 9.4 on page 121](#)).

### PSD

PSD (Power Spectral Density) defines the distribution of a VDSL line's power in the frequency domain. A PSD mask is a template that specifies the maximum allowable PSD for a line.

### Frequency Band Plan

Each VDSL mode operates in a different frequency band allocation, resulting in different upstream and downstream speeds. Your VES switch automatically changes the band plan based on the loop condition and loop length.

Band plans include an optional band (between 25 kHz and 276 kHz) controlled by "limit PSD mask". The optional band is used for upstream transmission which is to be negotiated during line initiation. A sample of limit PSD mask and associated frequency band is shown next.

**Table 26** Limit PSD Mask

TRANSMISSION MODE	CLASS MASK	US0 MASK	LIMIT MASK		FREQUENCY BAND
G.993.2 Annex A	998	EU-32	D-32	=	25 ~ 138 kHz
G.993.2 Annex A	998	EU-36	D-48	=	25 ~ 155.25 kHz
G.993.2 Annex A	998	EU-40	D-48	=	25 ~ 172.5 kHz
G.993.2 Annex A	998	....	...	=	...

## VDSL2 Profiles

Eight VDSL2 frequency profiles (8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a) are defined in G.993.2. They are based on each annex specifying spectral characters (Annexes A, B and C). Each profile covers certain settings and parameters, such as maximum aggregate transmit power. The higher-frequency profiles (17a and 30a) are mostly used to deliver high speed at shorter distances.

Note: At the time of writing, the Switch supports the Annex A with 8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a. The following table summarizes the VDSL2 profiles supported by the Switch.

**Table 27** VDSL2 Profiles on this Switch

FREQUENCY PLAN	PARAMETER	PARAMETER VALUE FOR PROFILE							
		8A	8B	8C	8D	12A	12B	17A	30A
Annex A	Maximum aggregate downstream transmit power (dBm)	+17.5	+20.5	+11.5	+14.5	+14.5	+14.5	+14.5	+14.5
	Index of highest supported downstream data-bearing sub-carrier (upper band edge frequency in MHz (informative))	1971 (8.5)	1971 (8.5)	1971 (8.5)	1971 (8.5)	1971 (8.5)	1971 (8.5)	N/A	N/A
	Index of highest supported upstream data-bearing sub-carrier (upper band edge frequency in MHz (informative))	1205 (5.2)	1205 (5.2)	1205 (5.2)	1205 (5.2)	2782 (12)	2782 (12)	N/A	N/A

## Configured Versus Actual Rate

You configure the maximum rate of an individual VDSL port by modifying its profile (see the [VDSL Line Profile Setup](#) screen) or assigning the port to a different profile (see the [VDSL Line Setup](#) screen). However, the actual rate varies depending on factors such as transmission range and interference.

## Impulse Noise Protection (INP)

Short impulses from external sources may cause bursts of errors which could impact the multimedia (ex. voice, video, or picture) quality. VDSL2 supports Impulse Noise Protection (INP) which provides the ability to correct errors regardless of the number of errors in an error DMT (Discrete Multi-Tone) symbol.

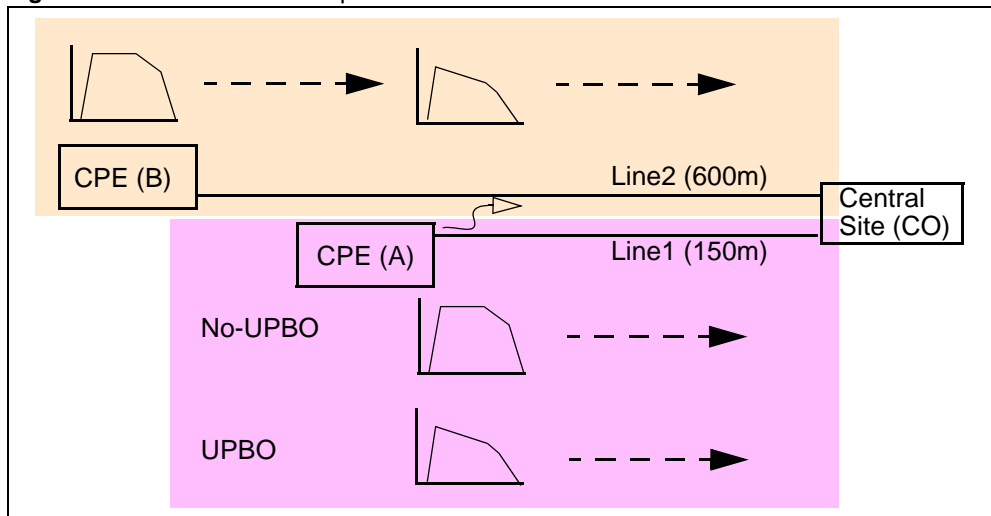
## UPBO

In a network with varying telephone wiring lengths, the PSD on each line is different. This causes crosstalk between the lines. Enable UPBO (Upstream Power Back Off) to allow the device to adjust the transmit PSD of all lines based on a reference line length. This mitigates the upstream crosstalk on shorter loops to longer loops. It allows the switch to provide better service in a network environment with telephone wiring of varying lengths.

An example is shown below. **Line 1** and **Line 2** are in the same cable binder. Crosstalk occurs when the signal flows and is near to **CPE (A)**'s location. Besides, higher **Line 1** PSD causes higher

interference to the **Line 2**. **CO** receives signal with higher attenuation. With UPBO enabled on the **CPE (A)**, it decreases the PSD level and reduces the crosstalk impact on long loops.

**Figure 51** UPBO Resolves Upstream Far-End Crosstalk



## DPBO

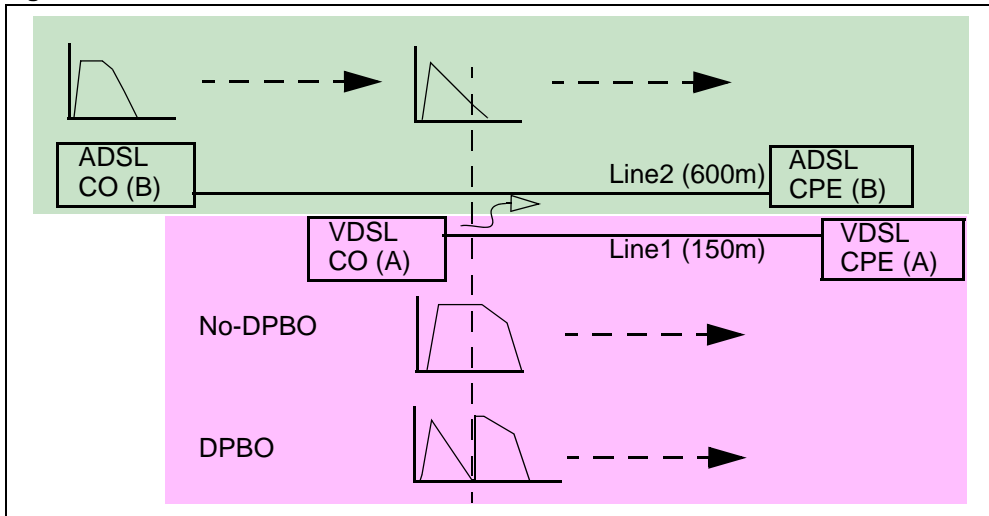
VDSL signal may interfere with other services (such as ISDN, ADSL or ADSL2 provided by other devices) on the same bundle of lines due to downstream far-end crosstalk. DPBO (Downstream Power Back Off) can reduce performance degradation by changing the PSD level on the VDSL switch(es) at street cabinet level.

ISDN in Europe uses a frequency range of up to 80 kHz, while ISDN in Japan uses a frequency range of up to 640 kHz. ADSL utilizes the 1.1 MHz band. Both ADSL2 and ADSL 2+ utilize the 2.2 MHz band.

An example is shown next. VDSL **Line 1** and ADSL **Line 2** are in the same binder. Crosstalk occurs when the ADSL signal flows from **CO (B)** and is near to **CO (A)**'s ONU (Optical Network Unit) location. Besides, higher **Line 1** PSD causes higher interference to the **Line 2**. **CPE (B)** receives

signal with higher attenuation. With DPBO enabled on the **CO (A)**, it decreases the PSD level and reduces the crosstalk impact on other service lines.

**Figure 52** DPBO Resolves Downstream Far-End Crosstalk



### UPBO/DPBO Electrical Length

The distance between a cabinet and the central office is an important parameter in UPBO/DPBO settings as we mentioned in the [DPBO](#) section on [page 99](#). The electrical length is used instead of the real physical distance according to G.997.1 format. Depending on the cable type the line used and physical line length, you can calculate the electrical length (in dB). For example, the distance is 1 kilometer and you use 24 AWG cable type, the electrical length 20.5 dB is suggested to be used.

The following table displays the calculation from a real length to an electrical length.

**Table 28** Real Length to Electrical Length

CABLE TYPE	REAL LENGTH TO ELECTRICAL LENGTH	A	B	C
22 AWG	= 16.2 x (cable length in kilometer)	0	0	0
24 AWG	= 20.5 x (cable length in kilometer)	0	1	0
26 AWG	= 25.8 x (cable length in kilometer)	0	1.0039065	-0.0039065

### Rate Adaption

Rate adaption is the ability of a device to adjust from the configured transmission rate to the attainable transmission rate automatically depending on the line quality. The VDSL transmission rate then stays at the new rate or adjusts if line quality improves or deteriorates.

The switch determines line quality using the Signal-to-Noise Ratio (SNR). SNR is the ration of signal power to noise power. A low SNR indicates poor line quality.

### SOS

SOS is a system for realizing emergency rate reduction. In a DSL system, especially in VDSL2 that uses wider frequency bandwidth and is deployed in the shorter loop than ADSL, far-end crosstalk (FEXT) may cause bursts of CRC errors and force CPE devices to retrain. SOS efficiently removes or

reduces crosstalk interference that leads to service interruption. When there is a burst of CRC errors, the receiver initiates a simple OLR (On-line reconfiguration) request for switching to a pre-determined adjustment transmission reference to the transmitter over an ROC (Robust Overhead Channel), then the transmitter sends a synchronous signal (SyncFlag). The receiver and transmitter synchronizes switching without exchanging the bit/gain table during SOS to avoid failure and new noise.

## G.INP

G.998.4 is also known as G.INP, which defines how data is retransmitted in an ADSL(+) or VDSL2 system to correct errors when impulse noise occurs. G.INP is similar to PhyR, Broadcom's proprietary physical layer retransmission scheme to improve impulse noise protection. In G.INP, the smallest amount of data that may be retransmitted is called DTU (Data Transfer Unit).

The differences between G.INP and PhyR includes:

- DTU is a set of an integer number of ATM cells or PTM 65B codewords.
- The overhead (indicator bit (IB), embedded operations channel (EOC)) information is carried on a separate latency path.
- A time stamp is appended to each DTU to provide better jitter control if necessary.

## RFI (Radio Frequency Interference)

RFI is induced noise on the lines by surrounding radio frequency electromagnetic radiation from sources such as AM and HAM radio stations. Since VDSL uses a much larger frequency range that overlaps with other radio frequency systems, signals from VDSL lines and other radio systems interfere with each other. To avoid performance degradation due to RFI, set the switch to not transmit VDSL signals in the RFI band.

## VDSL Profiles

A profile is a table that contains a list of pre-configured VDSL line settings or VDSL alarm threshold settings. Each VDSL port has one (and only one) line and alarm profile assigned to it at any given time.

Profiles allow you to configure VDSL ports efficiently. You can configure all of the VDSL ports with the same profile, thus removing the need to configure the VDSL ports one-by-one. You can also change an individual VDSL port by assigning it a different profile.

For example, you could set up different profiles for different kinds of accounts (for example, economy, standard and premium). Assign the appropriate profile to a VDSL port and it takes care of a large part of the port's configuration.

### 9.1.1 VDSL Profile Example

This example shows you the configuration relationships between VDSL templates, VDSL line profiles, VDSL line channel profiles, and subscriber ports.

Since each VDSL line may have different loop conditions, you need to configure several VDSL line profiles and channel profiles in the **VDSL Setup > VDSL Profile > VDSL Line Profile** and **VDSL Channel Profile** screens. For example, you have 3 VDSL line profiles (LinProfile-1, LinProfile-2 and LinProfile-3) and 3 channel profiles (ChanProfile-1, ChanProfile-2 and ChanProfile-3).

Secondly, you need to create several VDSL templates and configure their VDSL line profiles and channel profiles in the **VDSL Setup > VDSL Profile** screen. Examples are shown next.

**Table 29** VDSL Template Examples

VDSL TEMPLATE	VDSL LINE PROFILE	VDSL CHANNEL PROFILE
Template-A	LineProfile-2	ChanProfile-1
Template-B	LineProfile-1	ChanProfile-3
Template-C	LineProfile-2	ChanProfile-2
Template-D	LineProfile-3	ChanProfile-1

Then you can assign VDSL templates to VDSL ports in the **VDSL Setup > VDSL Line Setup** screen (see [Section 9.2 on page 103](#)).

**Table 30** VDSL Template Examples

PORT	PRIMARY TEMPLATE	FALLBACK TEMPLATE
1	Template-A	Template-B
2	Template-C	Template-D
3	Template-E	Template-F
4	Template-G	Template-H

## 9.1.2 Primary and Fallback VDSL Templates Example

On this Switch, you can specify a primary and a fallback VDSL template for each subscriber port. A subscriber port uses the parameters defined in the primary VDSL template when the line is initialized. When the actual line condition is too poor to use the primary template (for example, the defined minimum transmission rate cannot be reached), the Switch then uses the fallback template instead. You should select a looser fallback template for a line. See an example as shown next.

**Table 31** Primary and Fallback VDSL Template Settings Example

	PRIMARY TEMPLATE (P)	FALLBACK TEMPLATE (F)
<b>MIN RATE</b>	DS: 10 Mbps, US: 2 Mbps	DS: 9 Mbps, US: 1.5 Mbps
<b>TARGET SNR MARGIN</b>	6 dB	5 dB
<b>USO MASK</b>	EU32	EU128

The template **F** differs from templates **P** as follows.

- A lower transmission rate is allowed.
- Has higher tolerance against noise.
- Uses a wider band for USO mask.
- Using **F** can get higher bandwidth for upstream traffic when the line has poor quality or in a long distance.

## 9.2 VDSL Line Setup

Click **VDSL Setup** > **VDSL Line Setup** to display the screen as shown next. Use this screen to select the primary VDSL template, secondary VDSL template, and alarm template for each subscriber port.

Configure VDSL templates in **VDSL Setup** > **VDSL Profile** (see [Section 9.3 on page 104](#)). Configure VDSL alarm templates in **VDSL Setup** > **VDSL Alarm Profile** (see [Section 9.4 on page 121](#)).

**Figure 53** VDSL Line Setup

Port	Primary Template	Fallback Template	Alarm Template
1	DEFVAL	None	DEFVAL
2	DEFVAL	None	DEFVAL
3	DEFVAL	None	DEFVAL
4	DEFVAL	None	DEFVAL
5	DEFVAL	None	DEFVAL
6	DEFVAL	None	DEFVAL
7	DEFVAL	None	DEFVAL
8	DEFVAL	None	DEFVAL
9	DEFVAL	None	DEFVAL
10	DEFVAL	None	DEFVAL
11	DEFVAL	None	DEFVAL
12	DEFVAL	None	DEFVAL
13	DEFVAL	None	DEFVAL
...	...	...	...
24	DEFVAL	None	DEFVAL

Apply Cancel

The following table describes the labels in this screen.

**Table 32** VDSL Line Setup

LABEL	DESCRIPTION
Port	This is the port number of a subscriber port.
Primary Template	Select a VDSL template for a port. The template is used when the line is first initiated.
Fallback Template	Select a VDSL template for a port. This template is used when the line failed to be initialized using the primary template. See <a href="#">Primary and Fallback VDSL Templates Example on page 102</a> .
Alarm Template	Select a VDSL alarm template for a port. The Switch sends an SNMP trap (alarm) when a parameter value is over one of the pre-defined thresholds on the line.
Apply	Click this to save the settings to the Switch.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 9.3 VDSL Template Setup

The Switch supports one line profile and one channel profile configured in a VDSL template. Use this screen to add, modify or delete a VDSL template.

To configure or view VDSL templates, click **VDSL Setup** > **VDSL Profile** to display the screen as shown next.

Note: You can configure up to 60 VDSL templates.

**Figure 54** VDSL Template Setup

The following table describes the labels in this screen.

**Table 33** VDSL Template Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name to identify this template.
Line Profile	Select a line profile for this VDSL template. You can configure line profiles by clicking the <b>LineProfile</b> link in the right-top corner of the screen.
Channel Profile	Select a channel profile for this VDSL template. You can configure channel profiles by clicking the <b>ChanProfile</b> link in the right-top corner of the screen.
Inm Profile	Select an INM profile for this VDSL template. You can configure channel profiles by clicking the <b>InmProfile</b> link in the right-top corner of the screen.
Rate Adaption Ratio	
Channel1	This field displays the transmission rate distribution ratio between upstream and downstream traffic for channel 1 in this template.
Add	Click <b>Add</b> to save the new VDSL template to the Switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name for each configured VDSL template.
Line Profile	This field displays the line profile name configured in each VDSL template.
Channel Profile	This field displays the channel profile name configured in each VDSL template.



**Table 33** VDSL Template Setup (continued)

LABEL	DESCRIPTION
Applied Ports	This field displays the VDSL port number(s) to which this template is applied. You can apply templates to VDSL ports in the <b>VDSL Setup &gt; VDSL Line Setup</b> screen.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

### 9.3.1 VDSL Line Profile Setup

Click **VDSL Setup** > **VDSL Profile** and click the **LineProfile** link to open the screen as shown next. Use the screen to add, edit or delete a VDSL line profile.

**Figure 55** VDSL Line Profile Setup

The following table describes the labels in this screen.

**Table 34** VDSL Line Profile Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
VDSL2 Profile	Specify the VDSL2 profile you want to apply to this template. See <a href="#">VDSL2 Profiles</a> on page 98 for more information.

**Table 34** VDSL Line Profile Setup (continued)

LABEL	DESCRIPTION
Max SNR Margin	Enter the maximum SNR (Signal to Noise Ratio) margin allowed on the line. When the actual SNR margin is going to reach this specified value, this mechanism forces connected CPE device(s) to lower its transmission power level and maintains the actual SNR margin equal to or less than this value. Select <b>noLimit</b> to turn this mechanism off.
Target SNR Margin	Enter the target upstream and downstream SNR (Signal to Noise Ratio) margin.
Min SNR Margin	Enter the minimum upstream and downstream SNR margin accepted on the line to which this profile applies.
Bitswap	Select <b>On</b> to allow on-line bits and power (for example, margin) reallocation among the allowed sub-carriers without service interruption or errors. This helps to keep transmission data rate on a high SNR VDSL line.  Select <b>Off</b> to disable it.
Max Rx Power	Enter the maximum receiving power in dBm for <b>UpStream</b> traffic. Select <b>noLimit</b> if there is no limit.
Max Tx Power	Enter the maximum transmission power in dBm the Switch uses for <b>DownStream</b> traffic. Enter the maximum transmission power the CPE uses for <b>UpStream</b> traffic.
Min Overhead Rate	Enter the minimum transmission rate (4~248 kbps) reserved for a line's overhead channel. Both the Switch and CPE device use the overhead channel of a line to get VDSL transmission statistics with each other.
Limit PSD Mask	To reduce the impact of interference and attenuation, ITU-T G.993.2 specifies a limit PSD mask that limits the VDSL2 transmitters PSD at both downstream and upstream.
Transmission Mode	Select an appropriate transmission standard (according to your territory) you want to apply for this profile. At the time of writing, the Switch supports <b>G.993.2 Annex A</b> mode for countries which follow the North American VDSL2 standard.
ADSL/VDSL Protocol	Select the ADSL ( <b>G.992.1</b> , <b>G.992.2</b> , <b>G.992.3</b> , <b>G.992.5</b> , <b>ANSI</b> , and <b>ETSI</b> ) and VDSL ( <b>G.993.2</b> ) protocols this profile uses.
Class Mask	A class mask is a combination of several PSD masks according to the PSD mask types. The available options vary depending on your selection in the <b>Transmission Mode</b> field. At the time of writing, <b>998</b> is the only option in this field when you select <b>G.993.2 Annex A</b> in the <b>Transmission Mode</b> field.
Limit Mask	Select a downstream limit mask you want the Switch to use.
USO Mask	Select a limit mask you want the Switch to use for the upstream band 0.
UPBO	UPBO (Upstream Power Back-Off) mitigates far-end crosstalk (FEXT) caused by upstream transmission on shorter loops to longer loops. See <a href="#">UPBO</a> on <a href="#">page 98</a> .  Select <b>Auto</b> to enable UPBO and CPE devices' PSD adjustment based on the negotiation result with the Switch.  Select <b>Override</b> to force CPE devices to use the electrical length defined by the Switch (in the UPBOKL field below) to compute their UPBO. See <a href="#">UPBO/DPBO Electrical Length</a> on <a href="#">page 100</a> .  Select <b>Disable</b> to turn UPBO off.  Enter variable <b>A</b> and <b>B</b> values of upstream band 1 and band 2 for UPBO PSD mask calculation.
UPBOKL	Specify the electrical length (0~128 dB) of the cable between the Switch and CPE devices. See <a href="#">UPBO/DPBO Electrical Length</a> on <a href="#">page 100</a> .
UpStream Band 1 ~ 4	Specify 40~80.95 (dBm/Hz) for parameter <b>A</b> which defines the original band shape. Specify 0~40.95 for parameter <b>B</b> which defines the power back-off degree.
PM Mode	Select <b>allowTransitionsToIdle</b> to have the Switch or CPE devices autonomously enter an idle state for power management (PM).

**Table 34** VDSL Line Profile Setup (continued)

LABEL	DESCRIPTION
US0	Specify whether you want the Switch to automatically activate the upstream band 0 ( <b>Allow</b> ) or not ( <b>Disable</b> ) when necessary. Select <b>Allow</b> to have CPE and the Switch use the upstream band 0 for upstream traffic over long distances. If you select <b>Disable</b> , the CPE may not be able to transmit data over long distances.
Rate Adaptive	<p>This field displays downstream (DS) and upstream (US) rate adaptive settings.</p> <p><b>Manual</b> displays if the Switch fixes the transmission rate as the minimum net data rate and disables transmission rate adjustment. If the attainable speeds cannot match configured speeds, then the VDSL link may go down or link communications may be sporadic due to line errors and consequent retransmissions.</p> <p><b>AdaptInit</b> displays if the Switch keeps the transmission rate negotiated between the Switch and CPE devices. It ranges from the configured minimum to the maximum net data rate based on the initial line condition.</p> <p><b>Dynamic</b> displays if the Switch dynamically changes the transmission rate negotiated between the Switch and CPE devices during initialization as well as during SHOWTIME status.</p> <p><b>SOS</b> displays if the Switch uses the emergency rate adjustment system for immediate rate adjustment to reduce crosstalk noise.</p> <p>Click the <b>Modify</b> link to take you to a screen where you can configure detailed rate adaptive settings.</p>
MIB PSD MASK	<p>The MIB PSD mask allows you to further adjust PSD level for tones according to the limit PSD mask you have configured.</p> <p>This field displays how many break points are configured for the downstream (<b>DS</b>) and upstream (<b>US</b>) MIB PSD mask. For example, "<b>DS:4 BP US:5 BP</b>" displays after you have configured 4 break points for downstream and 5 break points for upstream in the MIB PSD mask.</p> <p>Click the <b>Modify</b> link to take you to a screen where you can configure the MIB PSD mask.</p>
DPBO	<p>This field displays whether DPBO is enabled or disabled in this profile.</p> <p>Click the <b>Modify</b> link to take you to a screen where you can configure detailed DPBO settings.</p>
RFI BAND	<p>This field displays the RFI band setting in this profile.</p> <p>Click the <b>Modify</b> link to take you to a screen where you can configure detailed RFI band settings.</p>
Virtual Noise	<p>This field displays whether virtual noise is enabled or disabled in the downstream and upstream transmissions.</p> <p>Click the <b>Modify</b> link to take you to a screen where you can configure detailed virtual noise settings.</p>
Add	Click <b>Add</b> to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name for this profile. Click a profile name in this field to edit that profile.
VDSL2 Profile	This field displays the VDSL2 profile(s) applied to a VDSL line profile.
SNR Margin	This field displays the configured upstream and downstream signal to noise ratio in decibels.

**Table 34** VDSL Line Profile Setup (continued)

LABEL	DESCRIPTION
Applied Ports	This field displays the VDSL port number(s) to which this profile is applied. You can apply a VDSL line profile to a VDSL template in the <b>VDSL Setup &gt; VDSL Profile &gt; VDSL Template Setup</b> screen.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

### 9.3.2 VDSL Line Profile Setup > Rate Adaptive

Click the **Modify** link next to the **Rate Adaptive** field in the **VDSL Line Profile Setup** screen to open the screen as shown next. Use the screen to configure detailed VDSL rate adaptive settings.

**Figure 56** VDSL Rate Adaptive Setup

The following table describes the labels in this screen.

**Table 35** VDSL Rate Adaptive Setup

LABEL	DESCRIPTION
DownStream	Configure the following settings for the Switch-to-CPEs direction.
UpStream	Configure the following settings for the CPEs-to-the-Switch direction.

**Table 35** VDSL Rate Adaptive Setup (continued)

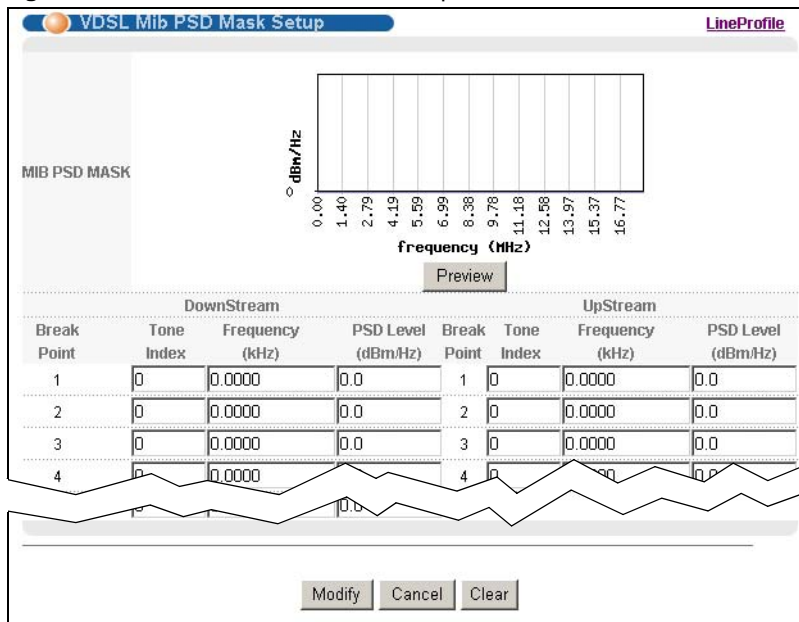
LABEL	DESCRIPTION
Rate Adaptive	<p>Select the rate adaptive modes for downstream and upstream transmissions.</p> <p>Select <b>Manual</b> to fix the transmit rate as the minimum net data rate and disable transmission rate adjustment. If the attainable speeds cannot match configured speeds, then the VDSL link may go down or link communications may be sporadic due to line errors and consequent retransmissions.</p> <p>Select <b>AdaptInit</b> to keep the transmit rate negotiated between CO and CPE devices. It ranges from the configured minimum to the maximum net data rate based on the initial line condition.</p> <p>Select <b>Dynamic</b> to dynamically change the transmission rate negotiated between the Switch and CPE devices during initialization as well as during SHOWTIME status.</p> <p>Select <b>SOS</b> to use the emergency rate adjustment system for immediate rate adjustment to reduce crosstalk noise.</p>
DynamicDepth	<p>Select <b>Enable</b> to allow the Switch to dynamically change interleaving depth for downstream or upstream traffic. In addition, this enables the Switch to change the lower and upper boundaries of the net data rate and improve the ability of SRA (Seamless Rate Adaptation). Alternatively, select <b>Disable</b> to have the Switch use a fixed interleaving depth.</p>
Up-Shift SNR Margin	<p>Enter the number of decibels (dB) for the line's up-shift SNR margin threshold. When the line's signal-to-noise margin goes above this number, the Switch attempts to use a higher transmission rate.</p>
Up-Shift Time	<p>Enter the number of seconds the Switch has to wait before using a higher transmission rate when the line's SNR margin is over the up-shift SNR margin threshold.</p>
Down-Shift SNR Margin	<p>Enter the number of decibels (dB) for the line's down-shift SNR margin threshold. When the line's signal-to-noise margin goes below this number, the Switch attempts to use a lower transmission rate.</p>
Down-Shift Time	<p>Enter the number of seconds the Switch waits before using a lower transmission rate when the line's SNR margin is less the down-shift SNR margin threshold.</p>
Modify	<p>Click this to save the settings to the Switch and return to the previous screen.</p>
SOS Time	<p>Specify the time interval (from 64 to 16320) at which the Switch initiates an SOS request.</p>
SOS CRC	<p>Specify the maximum number of CRC errors which are allowed during the specified SOS time interval before the Switch initiates an SOS request.</p>
SOS nTones	<p>Specify the maximum percentage (from 0 to 100) of persistently degraded tones in the MEDLEY set which are allowed during the specified SOS time interval before the Switch initiates an SOS request.</p>
SOS Max	<p>Specify the maximum number (from 0 to 15) of successful SOS processes which are allowed within 120 seconds before the Switch goes to the L3 link state. An SOS process is considered successful when the Switch receives a synchronous signal (SyncFlag).</p>
SOS Multi-Step Tones	<p>Select to adjust bits for all tones in an SOS request.</p>
ROC enable	<p>A ROC (robust overhead channel) is a latency path that carries only overhead data.</p> <p>Select <b>Enable</b> to use a ROC to transmit SOS information to ensure that the message can be received correctly. Otherwise, select <b>Disable</b>.</p>
ROC SNR Margin	<p>Specify the (Signal to Noise Ratio) margin allowed for a robust overhead channel. When the actual SNR margin is going to reach this specified value, a robust overhead channel is negotiated for reliable transmission.</p>
ROC min INP	<p>Specify the level of impulse noise (burst) protection for a robust overhead channel. Select a number between 0 and 16.</p>

**Table 35** VDSL Rate Adaptive Setup (continued)

LABEL	DESCRIPTION
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.

### 9.3.3 VDSL Line Profile Setup > MIB PSD Mask

Click the **Modify** link next to the **MIB PSD MASK** field in the **VDSL Line Profile Setup** screen to open the screen as shown next. Use this screen to adjust PSD levels for tones based on the scope down the limit PSD mask you have configured.

**Figure 57** VDSL MIB PSD Mask Setup

The following table describes the labels in this screen.

**Table 36** VDSL MIB PSD Mask Setup

LABEL	DESCRIPTION
MIB PSD Mask	This displays the PSD mask result in a graph. The MIB PSD mask is defined only within the operating bands and lies at or below the limit PSD mask. You may choose not to specify a MIB PSD mask for one or both transmission directions or in specific bands of the operating bands.
Preview	Click this to display the PSD mask result in the graph you configured at the bottom of the screen.
DownStream	Configure the following settings for the Switch-to-CPEs direction.
UpStream	Configure the following settings for the CPEs-to-the-Switch direction.
Break Point	This index number identifies each incremental break point.
Tone Index	A tone is a sub-channel of VDSL band. DMT divides VDSL bands into many 4.3125 kHz tones. Enter an increased number (than previous row) from 0 to 4096 in this field that is also the horizontal of the <b>MIB PSD Mask</b> graph.

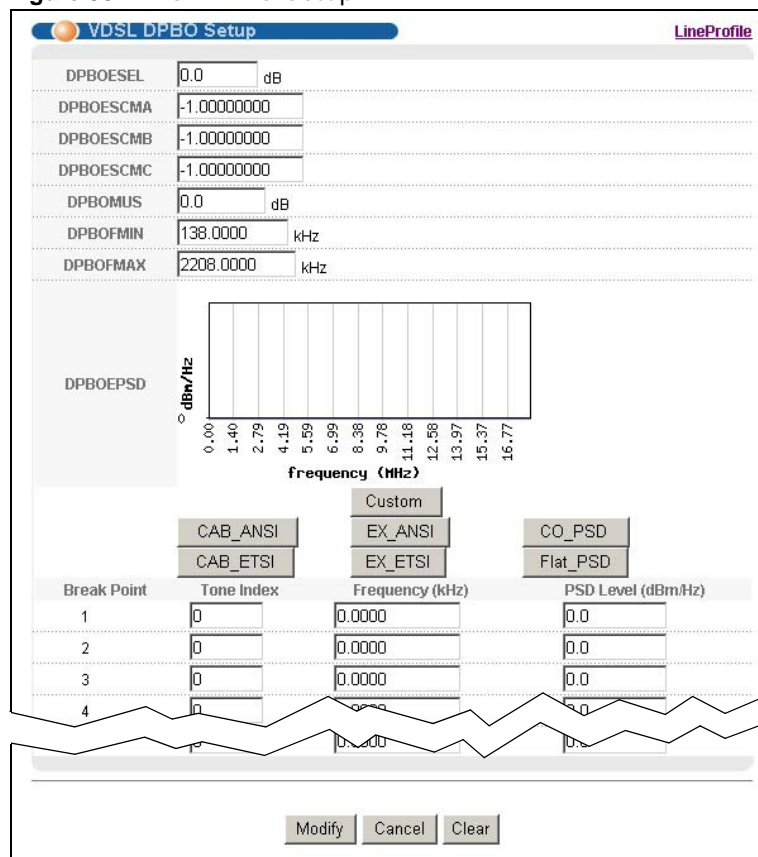
**Table 36** VDSL MIB PSD Mask Setup (continued)

LABEL	DESCRIPTION
Frequency (kHz)	This read-only field displays a frequency that equals the tone index multiple 4.3125 dBm/Hz. This field automatically calculates after a <b>Tone Index</b> value is entered.
PSD level (dBm/Hz)	Enter the PSD levels (-127.5–0 dBm/Hz) for your specified tones to restrict the transmit PSD to levels below these. Your input value will be displayed as the Y-axis of the <b>MIB PSD Mask</b> graph after you click <b>Preview</b> .
Modify	Click this to save the settings to the Switch and return to the previous screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.

### 9.3.4 VDSL Line Profile Setup > DPBO

Click the **Modify** link next to the **DPBO** field in the **VDSL Line Profile Setup** screen to open the screen as shown next. Use this screen to configure Downstream Power Back-Off (DPBO) settings. See [DPBO](#) on page 99.

**Figure 58** VDSL DPBO Setup





The following table describes the labels in this screen.

**Table 37** VDSL DPBO Setup

LABEL	DESCRIPTION
DPBOESEL	Specify the electrical length of the cable between the Switch and CPE devices. See <a href="#">UPBO/DPBO Electrical Length</a> on page 100.
DPBOESCMA, DPBOESCMB, DPBOESCMC	These parameters define a cable model that is used to describe the frequency dependent loss of exchange-side cables.
DPBOMUS	This defines the assumed minimum usable receives PSD mask (in dBm/Hz) for exchange based services, used to modify parameter DPBOFMAX defined below. Enter from 0 to -127.5 dBm/Hz in steps of 0.5 dB.
DPBOFMIN	This defines the minimum frequency from which the DPBO shall be applied. Enter from 0 kHz to 8832 kHz in steps of 4.3125 kHz.
DPBOFMAX	This defines the maximum frequency at which DPBO may be applied. Enter from 138 kHz to 29997.75 kHz in steps of 4.3125 kHz.
DPBOEPSD	DPBOEPSD (Assumed Exchange PSD Mask) defines the PSD mask that is assumed to be exchanged at CO. Use this graph to view PSD level to frequency relationship. The horizontal is frequency in MHz and vertical is power level in dBm/Hz.  Click <b>Custom</b> to have the breakpoints and PSD levels configured in the bottom of the screen updated to this DPBOEPSD graph.  Alternatively, you can click one of the others ( <b>CAB_ANSI</b> , <b>EX_ANSI</b> , <b>CO_PSD</b> , <b>CAB_ETSI</b> , <b>EX_ETSI</b> , <b>Flat_PSD</b> ) to use a pre-defined PSD mask.
DPBOESEL	Specify the electrical length of the cable between the Switch and CPE. See <a href="#">UPBO/DPBO Electrical Length</a> on page 100.
Break Point	This index number identifies each incremental break point.
Tone Index	A tone is a sub-channel of a VDSL band. DMT divides VDSL bands into many 4.3125 kHz tones.  Enter an increased number (than previous row) from 0 to 4096 in this field that is also the horizontal of the DPBOEPSD graph.
Frequency (kHz)	This read-only field displays a frequency that equals the tone index multiple 4.3125 dBm/Hz. This field automatically calculates after a <b>Tone Index</b> value is entered.
PSD level (dBm/Hz)	Enter the PSD level for the Y-axis of DPBOEPSD graph.
Modify	Click this to save the settings to the Switch and return to the previous screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.

### 9.3.5 VDSL Line Profile Setup > RFI Band

Click the **Modify** link next to the **RFI BAND** field in the **VDSL Line Profile Setup** screen to open the screen as shown next. Use this screen to specify the RFI bands through which the Switch and

VDSL CPE devices should avoid to transmit data according to your location. See [RFI \(Radio Frequency Interference\)](#) on page 101.

**Figure 59** VDSL RFI Setup

Band	Tone Index	Start		Stop	
		Frequency (kHz)	Tone Index	Frequency (kHz)	Tone Index
1	0	0.0000	0	0.0000	
2	0	0.0000	0	0.0000	
3	0	0.0000	0	0.0000	
4	0	0.0000	0	0.0000	
5	0	0.0000	0	0.0000	
6	0	0.0000	0	0.0000	
7	0	0.0000	0	0.0000	
8	0	0.0000	0	0.0000	
9	0	0.0000	0	0.0000	
10	0	0.0000	0	0.0000	
11	0	0.0000	0	0.0000	
12	0	0.0000	0	0.0000	
13	0	0.0000	0	0.0000	
14	0	0.0000	0	0.0000	
15	0	0.0000	0	0.0000	

Modify Cancel Clear

The following table describes the labels in this screen.

**Table 38** VDSL RFI Setup

LABEL	DESCRIPTION
Start	Use these columns below this field to specify the starting frequencies for each RFI band.
Stop	Use these columns below this field to specify the ending frequencies for each RFI band.
Band	This index number identifies each RFI Band.
Tone Index	A tone is a sub-channel of a VDSL band. DMT divides VDSL bands into many 4.3125 kHz tones. Enter an increased number (than previous row) from 0 to 4096.
Frequency (kHz)	This read-only field displays a frequency that equals the tone index multiple 4.3125 dBm/Hz. This field automatically calculates after a <b>Tone Index</b> value is entered.
Modify	Click this to save the settings to the Switch and return to the previous screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.

### 9.3.6 VDSL Line Profile Setup > Virtual Noise

Click the **Modify** link next to the **Virtual Noise** field in the **VDSL Line Profile** Setup screen to open the screen as shown next. Use the screen to configure VDSL virtual noise settings for a VDSL line profile.

**Figure 60** VDSL Virtual Noise Setup

DownStream				UpStream			
<input type="radio"/> Enable <input checked="" type="radio"/> Disable				<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Break Point	Tone Index	Frequency (kHz)	Noise Level (dBm/Hz)	Break Point	Tone Index	Frequency (kHz)	Noise Level (dBm/Hz)
1	0	0.0000	0	1	0	0.0000	0
2	0	0.0000	0	2	0	0.0000	0
3	0	0.0000	0	3	0	0.0000	0
4	0	0.0000	0	4	0	0.0000	0
5	0	0.0000	0	5	0	0.0000	0
31	0	0.0000	0				
32	0	0.0000	0				

The following table describes the labels in this screen.

**Table 39** VDSL Virtual Noise Setup

LABEL	DESCRIPTION
Virtual Noise	This displays the virtual noise setting result in a graph.  If there is too much noise on a line, the allowed line speed may be reduced or the line may not initialize. Virtual noise is the noise allowed on the line before the first line speed adjustment occurs. Switch then uses a lower data rate on tones which you added a noise level for the line initialization. A lower data rate increases a line's stability and avoid the line being easily dropped when actual noise occurs.
Preview	Click this to update the virtual noise setting result according to your setting configured at the bottom of the screen.
Downstream, Upstream	Select whether you want to enable virtual noise ( <b>Enable</b> ) or not ( <b>Disable</b> ) for downstream and upstream transmissions.  Note: For a poor quality subscriber line, you should enable this and configure virtual noise on tones where noise may occur.  Note: The higher the virtual noise, the lower the line speed.
Break Point	This index number identifies each incremental break point.

**Table 39** VDSL Virtual Noise Setup (continued)

LABEL	DESCRIPTION
Tone Index	A tone is a sub-channel of VDSL band. DMT divides VDSL bands into many 4.3125 kHz tones.  Enter an increased number (than previous row) from 0 to 4096 in this field that is also the horizontal of the DPBOEPSD graph.
Frequency (kHz)	This read-only field displays a frequency that equals the tone index multiple 4.3125 dBm/Hz. This field automatically calculates after a <b>Tone Index</b> value is entered.
Noise level (dBm/Hz)	Enter the noise level for the specified tone(s) where you expect noise may occur. This setting is then reflected in the Y-axis of the virtual noise graph after you click <b>Preview</b> .
Modify	Click this to save the settings to the Switch and return to the previous screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.

### 9.3.7 VDSL Channel Profile Setup

Click the **ChanProfile** link at the top-right corner of the **VDSL Template Setup** screen to open the screen shown below. Use this screen to view, add, modify and delete VDSL channel profiles.

**Figure 61** VDSL Channel Profile Setup

The following table describes the labels in this screen.

**Table 40** VDSL Channel Profile Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
DownStream	The parameters in this column relate to downstream transmissions.
Upstream	The parameters in this column relate to upstream transmissions.

**Table 40** VDSL Channel Profile Setup (continued)

LABEL	DESCRIPTION
Net Data Rate	Type maximum and minimum upstream/downstream transmission rates in kbps for this profile.
MaxInterleave Delay	Type the number of milliseconds of interleave delays used for downstream and upstream transmissions. It is recommended that you configure the same latency delays for both upstream and downstream.
Min INP	Specify the level of impulse noise (burst) protection for a slow (or interleaved) channel. Select a number between 0 and 16.  This parameter is defined as the number of consecutive DMT symbols or fractions thereof. The number of symbols decides how long in one period errors can be completely corrected. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may impact multimedia data receiving quality.
Min INP8	Specify the level of impulse noise (burst) protection for a slow (or interleaved) channel for VDSL2 profile 30a. Enter a number between 0 and 16.  The DMT symbols with a sub-carrier spacing for DS/US min INP8 is 8.625 kHz (DS/US min INP is 4.3125 kHz).
PhyR	Select <b>Enable</b> to use the VDSL physical layer for data re-transmission when impulse noise occurs. This helps to get better link connection quality.  Select <b>Disable</b> to turn this feature off.  Select <b>Auto</b> to have the Switch enable this feature when there is no impact to the data rate.
SOS Min Data Rate	Specify the minimum upstream/downstream data rates (guaranteed data rates) if you set the Switch to use SOS for immediate rate adjustment. The Switch drops the line if the upstream or downstream data rate goes down below the set data rate.
GINP	This field displays the upstream/downstream G.INP mode. Click <b>Modify</b> to change the G.INP settings.
Add	Click <b>Add</b> to save the new settings to the Switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name of a profile.
Payload Rate	This field displays the configured maximum upstream and downstream data transmission rates in megabits per second in a profile.
Min INP	This field displays the configured minimum upstream and downstream impulse noise protection levels in a profile.
Max Delay	This field displays the configured maximum upstream and downstream interleave delays in a profile.
Applied Ports	This field displays the VDSL port number(s) to which this profile is applied.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 9.3.8 VDSL G.INP Setup

Click the **Modify** link in the **VDSL Channel Profile Setup** screen to open the screen shown below. Use this screen to modify the G.INP settings.

**Figure 62** VDSL Channel Profile Setup > G.INP

	DownStream	UpStream
G.INP Mode	Preferred	Preferred
Effective Throughput	MAX 100032 MIN 192	MAX 100032 MIN 192
Net Data Rate(NDR)	MAX 100032	MAX 100032
Shine Ratio	0 /1000 * NDR	0 /1000 * NDR
LEFTR Threshold	0 /100 * NDR	0 /100 * NDR
Max Delay	8 ms	8 ms
Min Delay	0 ms	0 ms
Min INP	2 symbol	2 symbol
REIN Config	0 symbol 120 Hz	0 symbol 120 Hz

The following table describes the labels in this screen.

**Table 41** VDSL Channel Profile Setup > G.INP

LABEL	DESCRIPTION
DownStream	The parameters in this column relate to downstream transmissions.
Upstream	The parameters in this column relate to upstream transmissions.
G.INP Mode	Select G.INP retransmission mode. <b>Forbidden:</b> G.INP is disabled on the Switch. <b>Preferred:</b> G.INP is enabled if the far-end (CPE device) supports it. <b>Forced:</b> The VDSL connection can be established only if the far-end supports G.INP mode. <b>Test:</b> G.INP is enabled only in test mode.
Effective Throughput	Specify the maximum and minimum value allowed for the ETR (Effective Throughput Rate).
Net Data Rate(NDR)	Specify the maximum downstream/upstream net data rate.
Shine Ratio	Specifies the loss of data rate you predict to occur within 1 second due to SHINEs (Single high impulse noise events).  The valid values are all multiples of 0.001 and between 0 and 0.1.
LEFTR Threshold	Specify the lower rate limit (fraction of NDR). A Low Error Free Rate (LEFTR) defect is declared when the rate falls below the threshold.
Max Delay	Specify the maximum delay (from 1 to 63 in ms) that is added to the retransmission delay caused by retransmissions.
Min Delay	Specify the minimum delay (from 0 to 63 in ms) that is added to the retransmission delay caused by retransmissions.
Min INP	Specify the minimum level of impulse noise (burst) protection.

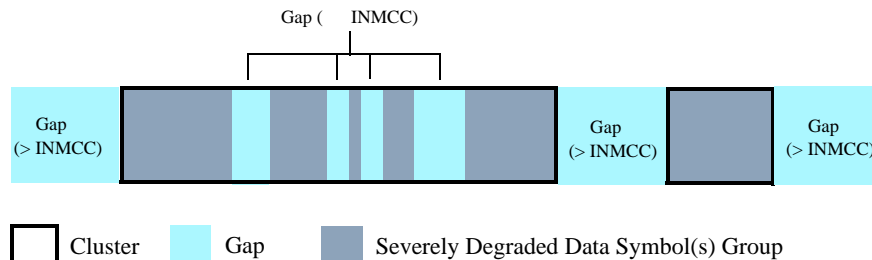
**Table 41** VDSL Channel Profile Setup > G.INP (continued)

LABEL	DESCRIPTION
REIN Config	Specify the major REIN (Repetitive Electrical Impulse Noise) with how many consecutive DMT symbols long and the operating frequency (100 or 120 Hz) in your territory. The Switch can completely correct the impulse noise by using the retransmission function.
Modify	Click <b>Modify</b> to save the new settings to the Switch.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.

### 9.3.9 VDSL INM Profile Setup

Click the **InmProfile** link at the top-right corner of the **VDSL Template Setup** screen to open the screen shown below.

In Impulse Noise Monitoring (INM), a cluster contains one or more groups of one single or consecutive severely degraded data symbols caused by impulse noise. Each cluster starts and ends with a severely degraded data symbol. Groups in a cluster are separated by a gap. A gap is a group of non-severely degraded data symbols between two severely degraded data symbols. Gaps between the groups in a cluster are smaller than or equal to the specified INM Cluster Continuation (INMCC). Gaps between the clusters are greater than the specified INMCC.

**Figure 63** INM Cluster Example

Use this screen to view, add, modify and delete VDSL INM profiles. An INM profile defines the control parameters used to generate the Equivalent INP (Eq INP or INP\_Eq) and Inter-Arrival Time (IAT) histograms. The IAT represents the number of data symbols from the start of one cluster to

the start of the next cluster. The Eq\_INP histogram shows the level of INP required to prevent data errors and the IAT histogram shows time intervals between the impulse noise events.

**Figure 64** Impulse Noise Monitor Setup

Name	NearEnd		FarEnd	
InpEqMode	0		0	
INMCC	0 symbol		0 symbol	
IAT Offset	3 symbol		3 symbol	
IAT Setp	0 symbol		0 symbol	
ISDD Sensitivity	0.0 dB		0.0 dB	

Name	InpEqMode	INMCC	IATO	IATS	Applied Ports	Delete
DEFVAL	0/0	0/0	3/3	0/0	1-24	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 42** Impulse Noise Monitor Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
NearEnd	The parameters in this column relate to upstream transmissions.
FarEnd	The parameters in this column relate to downstream transmissions.
InpEqMode	<p>Select the way of computing equivalent INP in this profile. See ITU-T G.993.2 for more information.</p> <p><b>0:</b> In this mode, the INMCC value is 0 and the cluster length (the number of data symbols from the first to the last severely degraded data symbols in a cluster) is used to generate the histogram. Each set of consecutive severely degraded data symbols is considered as a separate impulse noise event.</p> <p><b>1:</b> In this mode, the specified INMCC value and cluster length are used to generate the histogram. This provides an upper bound on the level of the required INP.</p> <p><b>2:</b> In this mode, the specified INMCC value and the number of the severely degraded data symbols in a cluster are used to generate the histogram. This provides a lower bound on the level of the required INP.</p> <p><b>3:</b> In this mode, the specified INMCC value, cluster length, the number of the severely degraded data symbols in a cluster and the number of gaps in a cluster are used to generate the histogram. This provides the best estimate of the required INP level.</p>
INMCC	Specify the cluster continuation value (0 to 64 DMT symbols) used for INM cluster indication.



**Table 42** Impulse Noise Monitor Setup (continued)

LABEL	DESCRIPTION
IAT Offset	Specify the IAT offset from 3 to 511 DMT symbols. This is to determine in which bin (category) of the IAT histogram the IAT is reported.  There are eight bins (0 to 7) in an IAT histogram. An IAT is logged in bin $y$ (where $y$ can be from 1 to 6) if the reported IAT value is in the range from $(\text{IAT Offset} + (y - 1) \times 2^{\text{IATStep}})$ to $((\text{IAT Offset} - 1) + (y) \times 2^{\text{IATStep}})$ . If an impulse event occurs at an interval less than the specified IAT offset, the IAT will be logged in bin 0 of the IAT histogram. Any IAT greater than or equal to $(\text{IAT Offset} + 6 \times 2^{\text{IATStep}})$ will be recorded in bin 7.
IAT Step	Specify the IAT step from 0 to 7. This is to determine in which bin (category) of the IAT histogram the IAT is reported.
ISDD Sensitivity	Specify the Impulse noise threshold of Severely Degraded symbol Detection from -12.8dB to +12.7 dB in steps of 0.1 dB. The smaller the value, the more sensitive the signal against impulse noise. For example, -12.8 dB is more sensitive to the symbol affected by impulse noise than +12.7 dB.
Add	Click <b>Add</b> to save the new settings to the Switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name of a profile.
InpEqMode	This field displays the configured upstream and downstream INPEq modes in a profile.
INMCC	This field displays the configured upstream and downstream INMCC values in a profile.
IATO	This field displays the configured upstream and downstream IAT offsets in a profile.
IATS	This field displays the configured upstream and downstream IAT steps in a profile.
Applied Ports	This field displays the VDSL port number(s) to which this profile is applied.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 9.4 VDSL Alarm Template Setup

Alarm profiles define VDSL port alarm thresholds. The device sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

Click **VDSL Setup** and **VDSL Alarm Profile** in the navigation panel to display the screen as shown. Use this screen to view, add, edit, and delete VDSL alarm profile templates. One VDSL alarm profile template specifies one VDSL line alarm profile and one VDSL channel alarm profile.

**Figure 65** VDSL Alarm Template Setup

The following table describes the labels in this screen.

**Table 43** VDSL Alarm Template Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Line Alarm Profile	Select a line alarm profile for this VDSL alarm profile template. You can configure line alarm profiles by clicking the <b>LineAlarmProfile</b> link in the top-right corner of the screen.
Channel Alarm Profile	Select a channel alarm profile for this VDSL alarm profile template. You can configure channel alarm profiles by clicking the <b>ChanAlarmProfile</b> link in the top-right corner of the screen.
Add	Click <b>Add</b> to save the new VDSL template to the Switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name for each configured VDSL template.
LineAlarmprofile	This field displays the line alarm profile name for each VDSL alarm profile template.
ChannelAlarmprofile	This field displays the channel alarm profile name for each VDSL alarm profile template.
Applied Ports	This field displays the VDSL port number(s) to which this template is applied.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 9.4.1 VDSL Line Alarm Profile Setup

Click the **LineAlarmProfile** link at the top-right corner of the **VDSL Alarm Template Setup** screen to display the screen as shown. Use this screen to view, add, edit, or delete a VDSL line alarm profile.

The device sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

**Figure 66** VDSL Line Alarm Profile Setup

The following table describes the labels in this screen.

**Table 44** VDSL Line Alarm Profile Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
VTUC	Configure the thresholds in this column for the Switch (VTUC).
VTUR	Configure the thresholds in this column for CPE devices (VTUR).
15 Minute FECS Threshold	Enter the number of Forward Error Correction Seconds (FECS) that are permitted to occur within 15 minutes.
15 Minute ES Threshold	Enter the number of Errored Seconds (ES) that are permitted to occur within 15 minutes.
15 Minute SES Threshold	Enter the number of Severely Errored Seconds (SES) that are permitted to occur within 15 minutes.
15 Minute LOSS Threshold	Enter the number of Loss Of Signals Seconds (LOSS) that are permitted to occur within 15 minutes.
15 Minute UAS Threshold	Enter the number of UnAvailable Seconds (UAS) that are permitted to occur within 15 minutes.
15 Minute LOFS Threshold	Enter the number of Loss Of Framing Seconds (LOFS) that are permitted to occur within 15 minutes.
15 Minute LPRS Threshold	Enter the number of times a Loss of Power Seconds (LPRS) is permitted to occur within 15 minutes.
15 Minute FailedFullInt Threshold	Enter the number of times a full initialization is allowed to fail within 15 minutes.

**Table 44** VDSL Line Alarm Profile Setup (continued)

LABEL	DESCRIPTION
Add	Click <b>Add</b> to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name for the alarm profile.
FECS	This field displays the number of Forward Error Correction Seconds (FECS) that are permitted to occur within 15 minutes.
ES	This field displays the number of Errored Seconds (ES) that are permitted to occur within 15 minutes.
SES	This field displays the number of Severely Errored Seconds (SES) that are permitted to occur within 15 minutes.
LOSS	This field displays the number of Loss Of Signal Seconds (LOSS) that are permitted to occur within 15 minutes.
UAS	This field displays the number of seconds the interface is permitted to be unavailable within 15 minutes.
Applied Ports	This field displays the VDSL port number(s) to which this profile is applied.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 9.4.2 VDSL Channel Alarm Profile Setup

Click the **ChanAlarmProfile** link at the top-right corner of the **VDSL Alarm Template Setup** screen to display the screen as shown. Use this screen to view, add, edit, modify a VDSL channel alarm profile.

The device sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

**Figure 67** VDSL Channel Alarm Profile Setup

VDSL Chan Alarm Profile Setup [AlarmTemplateProfile](#) [LineAlarmProfile](#)

Name: DEFVAL

15 Min Coding Violations Threshold: VTUC: 0, VTUR: 0

15 Min Corrected Blocks Threshold: VTUC: 0, VTUR: 0

Add Cancel Clear

Name	CV	Corrected	Applied Ports	Delete
DEFVAL	0/0	0/0	1-24	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

**Table 45** VDSL Channel Alarm Profile Setup

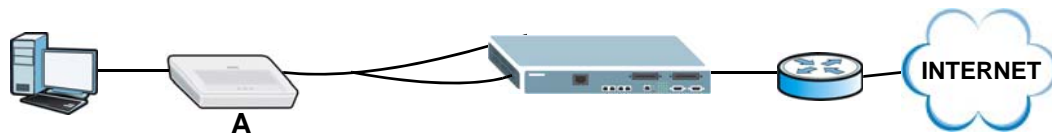
LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
VTUC	Configure the thresholds in this column for the Switch (VTUC).
VTUR	Configure the thresholds in this column for CPE devices (VTUR).
15Min CodeViolation Threshold	Enter the number of Code Violation (incorrect cyclic redundancy check) that are permitted to occur within 15 minutes.
15Min Corrected Blocks Threshold	Enter the number of error blocks that can be corrected within 15 minutes.
Add	Click <b>Add</b> to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Name	This field displays the descriptive name for the VDSL channel alarm profile.
CV	This field displays the number of Code Violation (incorrect cyclic redundancy check) that are permitted to occur within 15 minutes.
Corrected	This field displays the number of error blocks that can be corrected within 15 minutes.
Applied Ports	This field displays the VDSL port number(s) to which this profile is applied.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.

## 9.5 VDSL Bonding Setup

VDSL port bonding allows you to connect subscribers to an ISP using data streams spread over multiple DSL lines. The total available bandwidth for the subscriber then becomes the sum of the bandwidth available for each of the subscriber's line connections.

The next figure shows a subscriber using port bonding on two DSL lines between a CPE that supports VDSL bonding (A) (using a Y-connector) and the Switch to connect to the Internet.

**Figure 68** VDSL Port Bonding Example



Click **VDSL Setup** and **VDSL Bonding Setup** in the navigation panel to display the screen as shown. Use this screen to view, add, edit, and delete VDSL port bonding groups.

**Figure 69** VDSL Bonding Setup

Group ID	Name	Active	Port	Protocol	Mode	Group Rate	Port Rate	Template	Delete
<a href="#">B1</a>	Bonding1	Yes	22 23	PTM	1	100.032M/100.032M	50.016M/50.016M 50.016M/50.016M	DEFVAL	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 46** VDSL Bonding Setup

LABEL	DESCRIPTION
Active	Select the check box to enable this group.
Name	Enter a descriptive name for this group.
Group ID	Select an identifier number for this group from the drop-down list box.
Port	Select a pair of ports to be used by this DSL line group. A port can be in up to one bonding group at a time.
Template Profile	Select <b>Mode 1</b> and a single template profile to set a total data rate for the entire bonding group. The total data rate is divided equally for each port. Select <b>Mode 2</b> and select a separate template profile for each individual port in the bonding group to set each port's data rate independently.
Transmission Mode	Select a transmission standard ( <b>ATM</b> for ADSL or <b>PTM</b> for VDSL) to use for this group.
Add	Click <b>Add</b> to save the new group of DSL lines on which to use port bonding. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Group ID	This field displays a VDSL bonding group's ID. Click the ID to modify this group's settings.
Name	This field displays the name of the group.
Active	This field displays whether this group is enabled ( <b>Yes</b> ) or not ( <b>No</b> ).
Port	This field displays the port numbers in this group.
Protocol	This field displays the transmission mode protocol ( <b>PTM</b> or <b>ATM</b> ) this group uses.

**Table 46** VDSL Bonding Setup (continued)

LABEL	DESCRIPTION
Mode	<p>This field displays the template profile mode this group uses.</p> <p>This field displays <b>1</b> if a single template profile is set to have each port in the bonding group share a set total data rate equally.</p> <p>This field displays <b>2</b> if a separate template profile is set for each individual port in the bonding group. Each port uses a data rate independently.</p>
Group Rate	This field displays the upstream and downstream data rates for the entire bonding group.
Port Rate	This column displays the upstream and downstream data rates for individual ports in this group.
Template	This field displays the name of the template applied to this group.
Delete	Select the groups to remove in the <b>Delete</b> column and then click the <b>Delete</b> button to remove them.
Cancel	Click <b>Cancel</b> to clear the selected checkboxes in the <b>Delete</b> column.





The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

## 10.1 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

### 10.1.1 Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

## 10.1.2 VLAN Tagging Priority

When the Switch is IEEE 802.1Q VLAN-enabled, all incoming tagged traffic is forwarded according to the VLAN table on the Switch. If the incoming traffic is untagged, the Switch applies the VLAN rules based on the following priority:

MAC-based VLAN > Subnet-based VLAN > Protocol-based VLAN > PVID

## 10.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

### 10.2.1 GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

#### 10.2.1.1 GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

### 10.2.2 GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

**Table 47** IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.

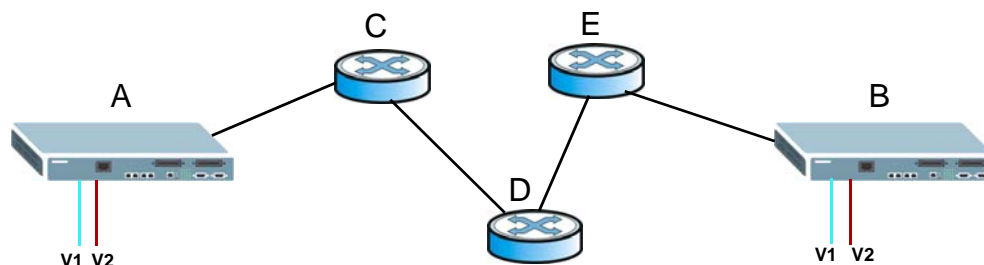
**Table 47** IEEE 802.1Q VLAN Terminology (continued)

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member

## 10.3 Port VLAN Trunking

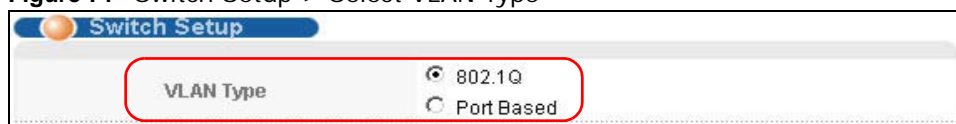
Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

**Figure 70** Port VLAN Trunking

## 10.4 Select the VLAN Type

Select a VLAN type in the **Basic Setting** > **Switch Setup** screen.

**Figure 71** Switch Setup > Select VLAN Type

## 10.5 Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

### 10.5.1 Static VLAN Status

See [Section 10.1 on page 129](#) for more information on Static VLAN. Click **Advanced Application > VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

**Figure 72** Advanced Application > VLAN: VLAN Status

Index	VID	Elapsed Time	Status
1	1	3:04:17	Static

The following table describes the labels in this screen.

**Table 48** Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the Switch.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the <b>Static VLAN</b> screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.

**Table 48** Advanced Application > VLAN: VLAN Status (continued)

LABEL	DESCRIPTION
Status	This field shows how this VLAN was added to the Switch.  <b>dynamic:</b> using GVRP <b>static:</b> added as a permanent entry <b>other:</b> added in another way such as via Multicast VLAN Registration (MVR)
Change Pages	Click <b>Previous</b> or <b>Next</b> to show the previous/next screen if all status information cannot be seen in one screen.

## 10.5.2 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See [Section 10.1 on page 129](#) for more information on static VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

**Figure 73** Advanced Application > VLAN > VLAN Detail

The screenshot shows the 'VLAN Detail' screen with a 'VLAN Status' link in the top right. The main table has columns for 'VID', 'Port Number' (with sub-columns 2-26), 'Elapsed Time', and 'Status'. For VID 1, all ports are marked 'U' and the elapsed time is 3:06:46, with a status of 'Static'.

VID	Port Number														Elapsed Time	Status
	2	4	6	8	10	12	14	16	18	20	22	24	26			
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	3:06:46	Static
	U	U	U	U	U	U	U	U	U	U	U	U	U	U		

The following table describes the labels in this screen.

**Table 49** Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the <b>VLAN Status</b> screen.
VID	This is the VLAN identification number that was configured in the <b>Static VLAN</b> screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as <b>T</b> , an untagged port is marked as <b>U</b> and ports not participating in a VLAN are marked as “—”.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch.  <b>dynamic:</b> using GVRP <b>static:</b> added as a permanent entry <b>other:</b> added in another way such as via Multicast VLAN Registration (MVR)

## 10.5.3 Configure a Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the Switch. See [Section 10.1 on page 129](#) for more information on static VLAN. To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

**Figure 74** Advanced Application > VLAN > Static VLAN

The following table describes the related labels in this screen.

**Table 50** Advanced Application > VLAN > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
VLAN Profile	Select a VLAN profile in which you can specify the action the Switch takes on incoming unknown multicast frames and whether to enable MAC address learning for this VLAN.
Port	The port number identifies the port you are configuring.

**Table 50** Advanced Application > VLAN > Static VLAN (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  <b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.
Control	Select <b>Normal</b> for the port to dynamically join this VLAN group using GVRP. This is the default selection.  Select <b>Fixed</b> for the port to be a permanent member of this VLAN group.  Select <b>Forbidden</b> if you want to prohibit the port from joining this VLAN group.
Tagging	Select <b>Tx Tagging</b> if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to change the fields back to their last saved values.
Clear	Click <b>Clear</b> to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled ( <b>Yes</b> ) or disabled ( <b>No</b> ).
Name	This field displays the descriptive name for this VLAN group.
VLAN Profile	This field displays the name of the VLAN profile applied to this VLAN.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 10.5.4 Configure a VLAN Profile

Click the **VLAN Profile** link at the top-right corner of the **Static VLAN** screen to open the screen shown below. Use this screen to view, add, modify and delete VLAN profiles.

**Figure 75** VLAN > Static VLAN > VLAN Profile

The screenshot shows the 'VLAN Profile' configuration interface. At the top, there's a title bar with 'VLAN Profile' and 'Static VLAN'. Below it, there are three rows of configuration options: 'Name' with a text input field, 'Mac Learning' with a checkbox, and 'Unknown Multicast' with a checkbox and the label 'flooding'. Below these options are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom, there is a table with columns: Index, Name, Mac Learning, Unknown Multicast, and Delete. The table contains one row with Index '1', Name 'DEFVAL', Mac Learning 'Yes', Unknown Multicast 'None', and a Delete checkbox. Below the table are two buttons: 'Delete' and 'Cancel'.

Index	Name	Mac Learning	Unknown Multicast	Delete
1	DEFVAL	Yes	None	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 51** VLAN > Static VLAN> VLAN Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Mac Learning	MAC address learning reduces outgoing broadcast traffic. Select the check box to enable MAC address learning in a VLAN.
Unknown Multicast	Specify the action to perform when the Switch receives an unknown multicast frame for a VLAN. Select <b>flooding</b> to send the frame(s) to all ports in the VLAN.
Add	Click <b>Add</b> to save the new settings to the Switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Index	This field displays the index number of a profile.
Name	This field displays the descriptive name of a profile. Click an index number to edit the profile.
Mac Learning	This field displays whether MAC address learning is enabled.
Unknown Multicast	This field displays the action the Switch takes on an unknown multicast frame received for the VLAN.
Delete	Check the profile(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkbox(es) in the <b>Delete</b> column.



## 10.5.5 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See [Section 10.1 on page 129](#) for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

**Figure 76** Advanced Application > VLAN > VLAN Port Setting

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
26	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 52** Advanced Application > VLAN > VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Port Isolation	<b>Port Isolation</b> allows each port to communicate only with the CPU management port and the dual personality GbE interfaces but not communicate with each other. This option is the most limiting but also the most secure.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
PVID	A Port VLAN ID (PVID) is a tag that the Switch adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1 and 4094 as the port VLAN ID.

**Table 52** Advanced Application > VLAN > VLAN Port Setting (continued)

LABEL	DESCRIPTION
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are <b>All</b> and <b>Tag Only</b> . Select <b>All</b> from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select <b>Tag Only</b> to accept only tagged frames on this port. All untagged frames will be dropped.
VLAN Trunking	Enable <b>VLAN Trunking</b> on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.6 Subnet Based VLANs

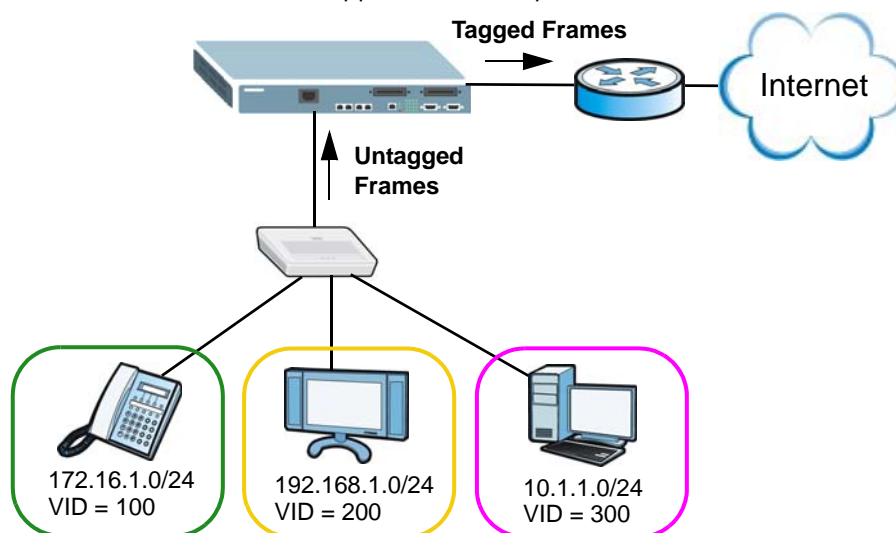
Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

For example, an ISP (Internet Services Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All

untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is video services receive the highest priority and data the lowest.

**Figure 77** Subnet Based VLAN Application Example



## 10.7 Configuring Subnet Based VLAN

Click **Subnet Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

**Figure 78** Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN

The following table describes the labels in this screen.

**Table 53** Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled, DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN.  Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Check this box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alpha numeric characters to identify this subnet based VLAN.
IP Type	Select to configure an IPv4 or IPv6 address.
IP	Enter the IPv4 or IPv6 address of the subnet for which you want to configure this subnet based VLAN.
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VID	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the <b>Advanced Application &gt; VLAN</b> screens.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.

**Table 53** Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to change the fields back to their last saved values.
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.

## 10.8 Protocol Based VLANs

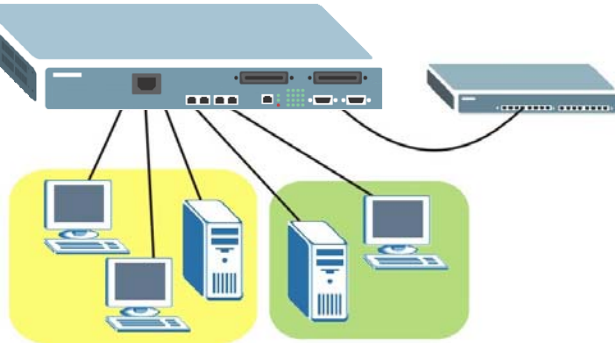
Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the Switch checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

Note: Protocol based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, port 1, 2, 3 and 4 belong to static VLAN 100, and port 4, 5, 6, 7 belong to static VLAN 120. You configure a protocol based VLAN A with priority 3 for ARP traffic received on port 1, 2 and 3. You also have a protocol based VLAN B with priority 2 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple

Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic, when they go through the uplink port to a backbone switch C.

**Figure 79** Protocol Based VLAN Application Example



## 10.9 Configuring Protocol Based VLAN

Click **Protocol Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Note: Protocol-based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

**Figure 80** Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN

The screenshot shows the 'Protocol Based VLAN' configuration interface. It includes a title bar with 'Protocol Based VLAN' and 'Vlan Port Setting'. The configuration fields are as follows:

- Active:** A checkbox that is currently unchecked.
- Port:** An empty text input field.
- Name:** An empty text input field.
- Ethernet-type:** Radio buttons for 'IP' (selected) and 'Others' (with a text input field for hex values).
- VID:** An empty text input field.
- Priority:** A dropdown menu currently set to '0'.

Below the configuration fields are 'Add' and 'Cancel' buttons. At the bottom, there is a table header with columns: Index, Active, Port, Name, Ethernet-type, VID, Priority, and Delete. Below the header are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 54** Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this protocol based VLAN.
Port	Type a port to be included in this protocol based VLAN.  This port must belong to a static VLAN in order to participate in a protocol based VLAN. See <a href="#">Chapter 10 on page 129</a> for more details on setting up VLANs.
Name	Enter up to 32 alpha numeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select <b>Others</b> and type the protocol number in hexadecimal notation. For example the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137.  Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the <b>Advanced Application &gt; VLAN</b> screens.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to change the fields back to their last saved values.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name the protocol based VLAN.
Ethernet Type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.10 Create an IP-based VLAN Example

This example shows you how to create an IP VLAN which includes ports 1, 4 and 8. Follow these steps:

- 1 Activate this protocol based VLAN.
- 2 Type the port number you want to include in this protocol based VLAN. Type **1**.
- 3 Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.
- 4 Select the protocol. Leave the default value **IP**.

- 5 Type the VLAN ID of an existing VLAN. In our example we already created a static VLAN with an ID of 5. Type **5**.
- 6 Leave the priority set to **0** and click **Add**.

**Figure 81** Protocol Based VLAN Configuration Example

The screenshot shows a configuration window for a Protocol Based VLAN. The title bar reads "Protocol Based VLAN" and "Vlan Port Setting". The configuration fields are as follows:

- Active:**
- Port:**
- Name:**
- Ethernet-type:**  IP  Others  (Hex)
- VID:**
- Priority:**

Below the form are "Add" and "Cancel" buttons. At the bottom of the window, there is a table with the following columns: Index, Active, Port, Name, Ethernet-type, VID, Priority, and Delete. Below the table are "Delete" and "Cancel" buttons.

To add more ports to this protocol based VLAN.

- 1 Click the index number of the protocol based VLAN entry. Click **1**
- 2 Change the value in the **Port** field to the next port you want to add.
- 3 Click **Add**.

## 10.11 Configuring MAC Based VLAN

MAC based VLANs allow you to group traffic into logical VLANs based on the MAC address you specify. When a frame is received on a port, the Switch checks if a tag is added already and the MAC address it came from. The untagged packets from the same MAC address(es) are then placed in the same MAC based VLAN. One advantage of using MAC based VLANs is that priority can be assigned to traffic from the same MAC address(es).

Click **MAC Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.



Note: MAC based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

**Figure 82** VLAN > VLAN Port Setting > MAC Based VLAN

The following table describes the labels in this screen.

**Table 55** VLAN > VLAN Port Setting > MAC Based VLAN

LABEL	DESCRIPTION
Active	Check this box to activate this MAC based VLAN.
Name	Enter up to 32 alpha numeric characters to identify this MAC based VLAN.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Enter the ID of a VLAN with which the untagged frames from the MAC address specified in this MAC based VLAN are tagged. This must be an existing VLAN which you defined in the <b>Advanced Application &gt; VLAN</b> screens.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to change the fields back to their last saved values.
Index	This is the index number identifying this MAC based VLAN. Click on any of these numbers to edit an existing MAC based VLAN.
Active	This field shows whether the MAC based VLAN is active or not.
Name	This field shows the name the MAC based VLAN.
MAC Address	This field shows the MAC address for this MAC based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this MAC based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this MAC based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.

## 10.12 Port Based VLAN Setup

Port based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port based VLANs are specific only to the Switch on which they were created.

Note: When you activate port based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.

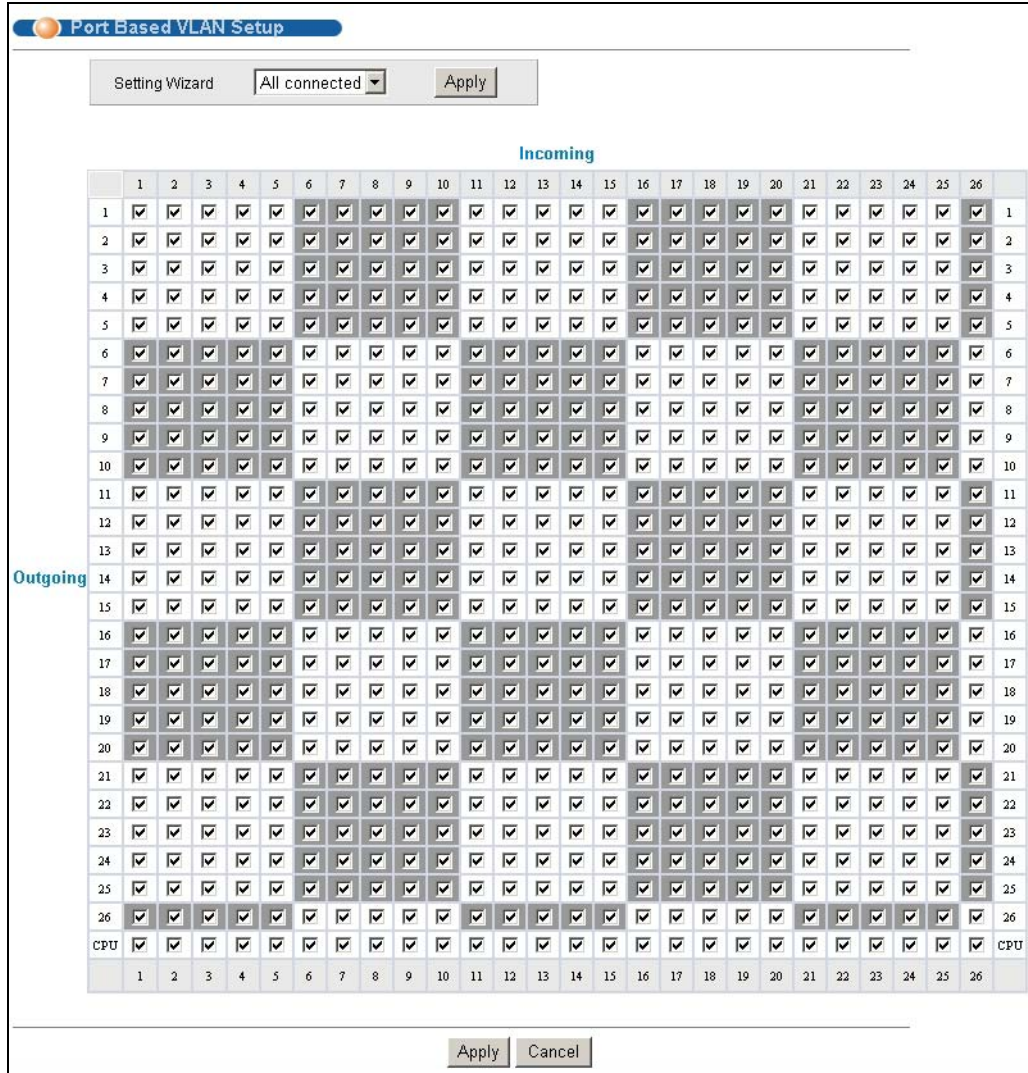
Note: In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

### 10.12.1 Configure a Port Based VLAN

Select **Port Based** as the **VLAN Type** in the **Basic Setting** > **Switch Setup** screen and then click **Advanced Application** > **VLAN** from the navigation panel to display the next screen.

Figure 83 Port Based VLAN Setup (All Connected)



**Figure 84** Port Based VLAN Setup (Port Isolation)

Port Based VLAN Setup

Setting Wizard    Port isolation ▼    Apply

		Incoming																												
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26			
Outgoing	1	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1	
	2	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
	3	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	3
	4	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	4
	5	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	5
	6	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	6
	7	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	7
	8	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	8
	9	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	9
	10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	10
	11	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	11
	12	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	12
	13	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	13
	14	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	14
	15	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	15
	16	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	16
	17	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	17
	18	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	18
	19	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	19
	20	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	20
	21	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	21
	22	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	22
	23	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	23
	24	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	24
	25	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	25
	26	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	26
CPU	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	CPU	

Apply Cancel

The following table describes the labels in this screen.

**Table 56** Port Based VLAN Setup

label	Description
Setting Wizard	<p>Choose <b>All connected</b> or <b>Port isolation</b>.</p> <p><b>All connected</b> means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure.</p> <p><b>Port isolation</b> means that each VDSL port can only communicate with the CPU management port and the uplink ports and cannot communicate with each other. All incoming ports are selected while only the CPU and uplink outgoing ports are selected. This option is the most limiting but also the most secure.</p> <p>After you make your selection, click <b>Apply</b> (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click <b>Apply</b> at the bottom of the screen.</p>
Incoming	<p>These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). <b>CPU</b> refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.</p>
Outgoing	<p>These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. <b>CPU</b> refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.</p>
Apply	<p>Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click <b>Cancel</b> to begin configuring this screen afresh.</p>

## 10.13 VLAN Counter

Click the **VLAN Counter** link in the **VLAN Status** screen to display the screen as shown next. Use this screen to view the frame statistics on uplink Ethernet ports.

**Figure 85** Vlan Counter

Vlan Info	Vlan Id.	1
	System up time:	0:08:45
Port Info	Port number	3
	Direction	RX TX
Packet	KBs/s	0.0 0.0
	Bytes	0 0
	Packets	0 0
	Multicast	0 0
	Broadcast	0 0
Distribution	64	0 0
	65 to 127	0 0
	128 to 255	0 0
	256 to 511	0 0
	512 to 1023	0 0
	1024 to 1518	0 0
	Giant	0 0

The following table describes the labels in this screen.

**Table 57** Vlan Counter

Label	Description
VID	Enter a VLAN identification number.
Port	Enter an uplink Ethernet port number.
Start	Click this to start the frame statistics calculation for the specified VLAN, port, and direction.
Stop	This button appears after you start a frame statistics calculation. Click this to stop the frame statistics calculation and reset the <b>VID</b> and <b>Port</b> fields to their default settings.
Update	This button appears after you start a frame statistics calculation. Click this to get the latest frame statistics for the port shown in this screen.
Clear	This button appears after you start a frame statistics calculation. Click this to have the frame statistics for the port reset.
Vlan Info	
Vlan Id.	This field displays the VLAN ID you are viewing.
System up time	This field shows the total amount of time the Switch has been up.
Port Info	
Port number	This field displays the port number you are viewing.
Direction	

**Table 57** Vlan Counter (continued)

Label	Description
Direction	<del>This field displays the traveling direction of the packets you are viewing.</del>
Packet	This field shows the number of transmitted and received frames on this port
KBs/s	This field shows the number kilobytes per second the Switch has transmitted and received on this port.
Bytes	This field shows the number of bytes the Switch has transmitted and received.
Packets	The following fields display detailed information about packets the Switch has transmitted and received.
Multicast	This field shows the number of good multicast packets the Switch has transmitted and received.
Broadcast	This field shows the number of good broadcast packets the Switch has transmitted and received.
Distribution	
64	This field shows the number of packets (including bad packets) transmitted and received that were 64 octets in length.
65 to 127	This field shows the number of packets (including bad packets) transmitted and received that were between 65 and 127 octets in length.
128 to 255	This field shows the number of packets (including bad packets) transmitted and received that were between 128 and 255 octets in length.
256 to 511	This field shows the number of packets (including bad packets) transmitted and received that were between 256 and 511 octets in length.
512 to 1023	This field shows the number of packets (including bad packets) transmitted and received that were between 512 and 1023 octets in length.
1024 to 1518	This field shows the number of packets (including bad packets) transmitted and received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets (including bad packets) transmitted and received that were between 1519 octets and the maximum frame size.  The maximum frame size varies depending on your switch model. See <a href="#">Chapter 47 on page 381</a> .

# Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

## 11.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

## 11.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch. See [Chapter 19 on page 191](#) for more information about MAC limit.

Click **Advanced Application** > **Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

**Figure 86** Advanced Application > Static MAC Forwarding

The screenshot displays the 'Static MAC Forwarding' configuration interface. It features a form with the following fields:

- Active:** A checkbox.
- Name:** A text input field.
- MAC Address:** A text input field with six segments separated by colons (e.g., [ ] : [ ] : [ ] : [ ] : [ ] : [ ]).
- VID:** A text input field.
- Port:** A text input field.

Below the form are three buttons: **Add**, **Cancel**, and **Clear**. At the bottom of the screen, there is a table with the following columns: **Index**, **Active**, **Name**, **MAC Address**, **VID**, **Port**, and **Delete**. Below the table are two buttons: **Delete** and **Cancel**. In the top right corner, there is a **Paging** control with **Prev**, **Next**, and **p. 1** (with a dropdown arrow).



The following table describes the labels in this screen.

**Table 58** Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. <b>Note: Static MAC addresses do not age out.</b>
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click <b>Add</b> to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields to their last saved values.
Clear	Click <b>Clear</b> to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active ( <b>Yes</b> ) or not ( <b>No</b> ). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.

# Static Multicast Forward Setup

Use these screens to configure static multicast address forwarding.

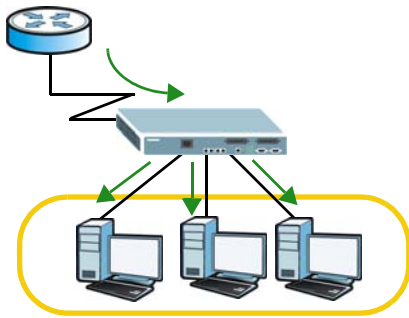
## 12.1 Static Multicast Forwarding Overview

A multicast MAC address is the MAC address of a member of a multicast group. A static multicast address is a multicast MAC address that has been manually entered in the multicast table. Static multicast addresses do not age out. Static multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

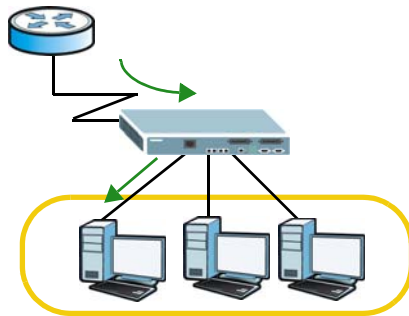
If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. You can configure this in the **Advanced Application > Multicast > Multicast Setting** screen (see [Section 24.3 on page 224](#)). [Figure 87](#) shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicast frames to

port(s) within a VLAN group. [Figure 88](#) shows frames being forwarded to devices connected to port 3. [Figure 89](#) shows frames being forwarded to ports 2 and 3 within VLAN group 4.

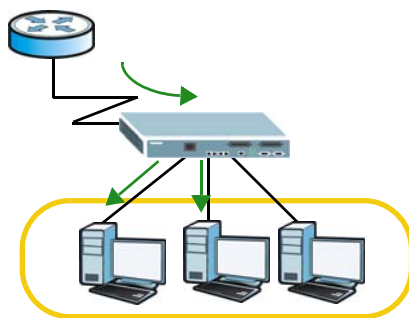
**Figure 87** No Static Multicast Forwarding



**Figure 88** Static Multicast Forwarding to A Single Port



**Figure 89** Static Multicast Forwarding to Multiple Ports



## 12.2 Configuring Static Multicast Forwarding

Use this screen to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

Click **Advanced Application > Static Multicast Forwarding** to display the configuration screen as shown.

**Figure 90** Advanced Application > Static Multicast Forwarding

The following table describes the labels in this screen.

**Table 59** Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Add	Click <b>Add</b> to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields to their last saved values.
Clear	Click <b>Clear</b> to begin configuring this screen afresh.
Index	Click an index number to modify a static multicast MAC address rule for port(s).
Active	This field displays whether a static multicast MAC address forwarding rule is active ( <b>Yes</b> ) or not ( <b>No</b> ). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.

**Table 59** Advanced Application > Static Multicast Forwarding (continued)

LABEL	DESCRIPTION
Pre. Page	Click this to show the previous screen if all entries cannot be seen in one screen.
Next Page	Click this to show the next screen if all entries cannot be seen in one screen.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

This chapter discusses MAC address port filtering.

## 13.1 Configure a Filtering Rule

Filtering means sifting traffic going through the Switch based on the source and/or destination MAC addresses and VLAN group (ID).

Click **Advanced Application > Filtering** in the navigation panel to display the screen as shown next.

**Figure 91** Advanced Application > Filtering

The following table describes the related labels in this screen.

**Table 60** Advanced Application > Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.
Action	Select <b>Discard source</b> to drop the frames from the source MAC address (specified in the <b>MAC</b> field). The Switch can still send frames to the MAC address.  Select <b>Discard destination</b> to drop the frames to the destination MAC address (specified in the <b>MAC</b> address). The Switch can still receive frames originating from the MAC address.  Select <b>Discard source</b> and <b>Discard destination</b> to block traffic to/from the MAC address specified in the <b>MAC</b> field.

**Table 60** Advanced Application > Filtering (continued)

LABEL	DESCRIPTION
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays <b>Yes</b> when the rule is activated and <b>No</b> when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Action	This field displays the filtering action.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkbox(es) in the <b>Delete</b> column.

# Spanning Tree Protocol

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

## 14.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

### 14.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

**Table 61** STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535



**Table 61** STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

## 14.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

## 14.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

**Table 62** STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.  Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

### 14.1.4 Multiple RSTP

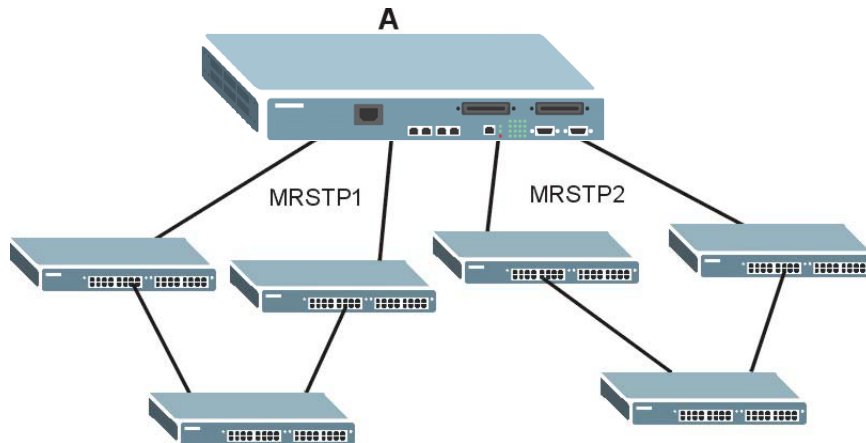
MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

To set up MRSTP, activate MRSTP on the Switch and specify which port(s) belong to which spanning tree.

Note: Each port can belong to one STP tree only.

**Figure 92** MRSTP Network Example



### 14.1.5 Multiple STP

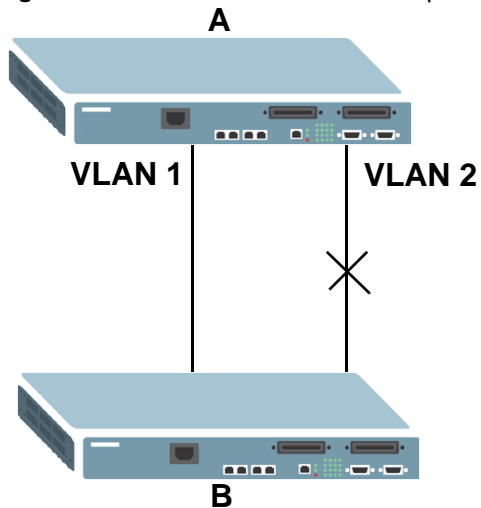
Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

### 14.1.5.1 MSTP Network Example

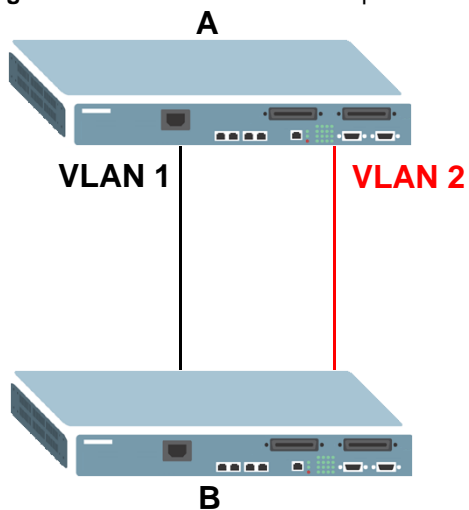
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

**Figure 93** STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

**Figure 94** MSTP Network Example



### 14.1.5.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

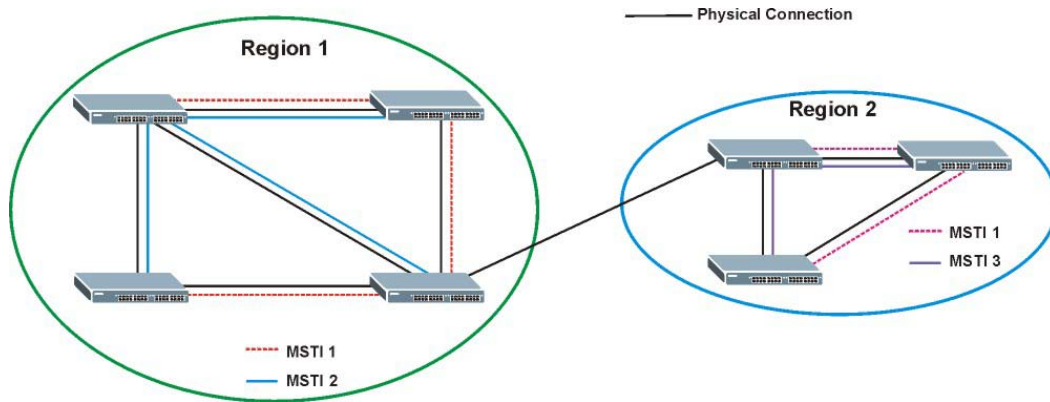
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

### 14.1.5.3 MST Instance

An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

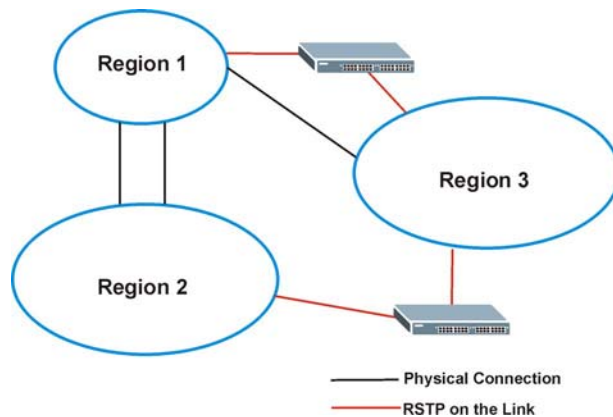
**Figure 95** MSTIs in Different Regions



### 14.1.5.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

**Figure 96** MSTP and Legacy RSTP Network Example



## 14.2 Spanning Tree Protocol Status Screen

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application** > **Spanning Tree Protocol** to see the screen as shown.

**Figure 97** Advanced Application > Spanning Tree Protocol

The screenshot shows the 'Spanning Tree Protocol Status' screen with the 'RSTP' mode selected. The screen displays a comparison between the local bridge and the root bridge across various parameters.

Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	0000-000000000000
Hello Time (second)	0	0
Max Age (second)	0	0
Forwarding Delay (second)	0	0
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times		0
Time Since Last Change		0:00:00

This screen differs depending on which STP mode (RSTP, MRSTP or MSTP) you configure on the Switch. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the Switch.

## 14.3 Spanning Tree Configuration

Use the **Spanning Tree Configuration** screen to activate one of the STP modes on the Switch. Click **Configuration** in the **Advanced Application** > **Spanning Tree Protocol**.

**Figure 98** Advanced Application > Spanning Tree Protocol > Configuration

The screenshot shows the 'Spanning Tree Configuration' screen with the 'Rapid Spanning Tree' mode selected. The screen includes 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 63** Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select <b>Rapid Spanning Tree</b> , <b>Multiple Rapid Spanning Tree</b> or <b>Multiple Spanning Tree</b> . See <a href="#">Section 14.1 on page 160</a> for background information on STP.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 14.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 14.1 on page 160](#) for more information on RSTP. Click **RSTP** in the **Advanced Application > Spanning Tree Protocol** screen.

**Figure 99** Advanced Application > Spanning Tree Protocol > RSTP

Port	Active	Priority	Path Cost
*	<input type="checkbox"/>		
25	<input type="checkbox"/>	128	4
26	<input type="checkbox"/>	128	4

The following table describes the labels in this screen.

**Table 64** Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click <b>Status</b> to display the <b>RSTP Status</b> screen (see <a href="#">Figure 100 on page 167</a> ).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP.  Note: You must also activate <b>Rapid Spanning Tree</b> in the <b>Advanced Application &gt; Spanning Tree Protocol &gt; Configuration</b> screen to enable RSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.  The lower the numeric value you assign, the higher the priority for this bridge.  Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

**Table 64** Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. 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. The allowed range is 4 to 30 seconds.  As a general rule:  Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Priority	Configure the priority for each port here.  Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see <a href="#">Table 61 on page 160</a> for more information.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 14.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 14.1 on page 160](#) for more information on RSTP.

Note: This screen is only available after you activate RSTP on the Switch.

**Figure 100** Advanced Application > Spanning Tree Protocol > Status: RSTP

Spanning Tree Protocol Status		
	Root	Our Bridge
Bridge ID	0000-000000000000	0000-000000000000
Hello Time (second)	0	0
Max Age (second)	0	0
Forwarding Delay (second)	0	0
Cost to Bridge	0	
Port ID	0x0000	0
Topology Changed Times		0
Time Since Last Change		0:00:00

The following table describes the labels in this screen.

**Table 65** Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click <b>Configuration</b> to specify which STP mode you want to activate. Click <b>RSTP</b> to edit RSTP settings on the Switch.
Bridge	<b>Root</b> refers to the base of the spanning tree (the root bridge). <b>Our Bridge</b> is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for <b>Root</b> and <b>Our Bridge</b> if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).  <b>Note: The listening state does not exist in RSTP.</b>
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

## 14.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 14.1 on page 160](#) for more information on MRSTP.

**Figure 101** Advanced Application > Spanning Tree Protocol > MRSTP

Tree	Active	Bridge Priority	Hello Time	MAX Age	Forwarding Delay
1	<input type="checkbox"/>	32768	2 seconds	20 seconds	15
2	<input type="checkbox"/>	32768	2 seconds	20 seconds	15

Port	Active	Priority	Path Cost	Tree
*	<input type="checkbox"/>			1
25	<input type="checkbox"/>	128	4	1
26	<input type="checkbox"/>	128	4	1

Apply Cancel



The following table describes the labels in this screen.

**Table 66** Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click <b>Status</b> to display the <b>MRSTP Status</b> screen (see <a href="#">Figure 100 on page 167</a> ).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree.  <b>Note:</b> You must also activate <b>Multiple Rapid Spanning Tree</b> in the <b>Advanced Application &gt; Spanning Tree Protocol &gt; Configuration</b> screen to enable MRSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.  The lower the numeric value you assign, the higher the priority for this bridge.  Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. 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. The allowed range is 4 to 30 seconds.  As a general rule:  <b>Note:</b> $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  <b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here.  Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see <a href="#">Table 61 on page 160</a> for more information.
Tree	Select which STP tree configuration this port should participate in.

**Table 66** Advanced Application > Spanning Tree Protocol > MRSTP (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 14.7 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 14.1 on page 160](#) for more information on MRSTP.

Note: This screen is only available after you activate MRSTP on the Switch.

**Figure 102** Advanced Application > Spanning Tree Protocol > Status: MRSTP

Bridge	Root	Our Bridge
Bridge ID	8000-001349000002	8000-001349000002
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times		0
Time Since Last Change		0:00:00

The following table describes the labels in this screen.

**Table 67** Advanced Application > Spanning Tree Protocol > Status: MRSTP

LABEL	DESCRIPTION
Configuration	Click <b>Configuration</b> to specify which STP mode you want to activate. Click <b>MRSTP</b> to edit MRSTP settings on the Switch.
Tree	Select which STP tree configuration you want to view.
Bridge	<b>Root</b> refers to the base of the spanning tree (the root bridge). <b>Our Bridge</b> is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for <b>Root</b> and <b>Our Bridge</b> if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).  <b>Note:</b> The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.

**Table 67** Advanced Application > Spanning Tree Protocol > Status: MRSTP (continued)

LABEL	DESCRIPTION
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

## 14.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 14.1.5 on page 162](#) for more information on MSTP.

**Figure 103** Advanced Application > Spanning Tree Protocol > MSTP

**Multiple Spanning Tree Protocol**
Status

---

**Bridge:**

Active	<input type="checkbox"/>	
Hello Time	<input type="text" value="2"/> seconds	
MAX Age	<input type="text" value="20"/> seconds	
Forwarding Delay	<input type="text" value="15"/> seconds	
Maximum hops	<input type="text" value="128"/>	
Configuration Name	<input type="text" value="0019cb000601"/>	
Revision Number	<input type="text" value="0"/>	

Apply Cancel

---

**Instance:**

Instance	<input type="text"/>	
Bridge Priority	<input type="text" value="32768"/>	
VLAN Range	Start <input type="text"/> End <input type="text"/>	Add Remove Clear
Enabled VLAN(s)	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>	

Port	Active	Priority	Path Cost
*	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
25	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
26	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>

Add Cancel

---

Instance	VLAN	Active Port	Delete
0	1-4094	-	Delete

Delete Cancel

The following table describes the labels in this screen.

**Table 68** Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click <b>Status</b> to display the <b>MSTP Status</b> screen (see <a href="#">Figure 104 on page 174</a> ).
Active	Select this to activate MSTP on the Switch. Clear this to disable MSTP on the Switch.  Note: You must also activate <b>Multiple Spanning Tree</b> in the <b>Advanced Application &gt; Spanning Tree Protocol &gt; Configuration</b> screen to enable MSTP on the Switch.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MaxAge	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. 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. The allowed range is 4 to 30 seconds. As a general rule:  Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-16.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance.  Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the <b>Start</b> field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the <b>End</b> field.  Next click: <ul style="list-style-type: none"> <li>• <b>Add</b> - to add this range of VLAN(s) to be mapped to the MST instance.</li> <li>• <b>Remove</b> - to remove this range of VLAN(s) from being mapped to the MST instance.</li> <li>• <b>Clear</b> - to remove all VLAN(s) from being mapped to this MST instance.</li> </ul>
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.

**Table 68** Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  <b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to add this port to the MST instance.
Priority	Configure the priority for each port here.  Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see <a href="#">Table 61 on page 160</a> for more information.
Add	Click <b>Add</b> to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 14.9 Multiple Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 14.1.5 on page 162](#) for more information on MSTP.

Note: This screen is only available after you activate MSTP on the Switch.

**Figure 104** Advanced Application > Spanning Tree Protocol > Status: MSTP

**Spanning Tree Protocol Status** Configuration RSTP MRSTP **MSTP**

**Spanning Tree Protocol: MSTP**

**CST**

Bridge	Root	Our Bridge
Bridge ID	0-000000000000	8000-000000000000
Hello Time (second)	0	2
Max Age (second)	0	20
Forwarding Delay (second)	0	15
Cost to Bridge	0	0
Port ID	0x0000	0x0000
Configuration Name	0019cb000601	
Revision Number	0	
Configuration Digest	AC36177F50283CD4B83821D8AB26DE62	
Topology Changed Times	0	
Time Since Last Change	0:00:00	

**Instance:**

Instance	VLAN
0	1-4094

**MSTI** 1

Bridge	Regional Root	Our Bridge
Bridge ID	0000-000000000000	8001-000000000000
Internal Cost	0	0
Port ID	0x0000	0x0000

The following table describes the labels in this screen.

**Table 69** Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click <b>Configuration</b> to specify which STP mode you want to activate. Click <b>MSTP</b> to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	<b>Root</b> refers to the base of the spanning tree (the root bridge). <b>Our Bridge</b> is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for <b>Root</b> and <b>Our Bridge</b> if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

**Table 69** Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	<b>Regional Root</b> refers to the base of the MST instance. <b>Our Bridge</b> is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for <b>Regional Root</b> and <b>Our Bridge</b> if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.

## Broadcast Storm Control

This chapter introduces and shows you how to configure the broadcast storm control feature.

### 15.1 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

Click **Advanced Application > Broadcast Storm Control** in the navigation panel to display the screen as shown next.

**Figure 105** Advanced Application > Broadcast Storm Control

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 70** Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.



**Table 70** Advanced Application > Broadcast Storm Control (continued)

LABEL	DESCRIPTION
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields.

# Mirroring

This chapter discusses port mirroring setup screens.

## 16.1 Port Mirroring Setup

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Click **Advanced Application > Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

**Figure 106** Advanced Application > Mirroring

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
1	<input type="checkbox"/>	Ingress ▼
2	<input type="checkbox"/>	Ingress ▼
3	<input type="checkbox"/>	Ingress ▼
4	<input type="checkbox"/>	Ingress ▼
5	<input type="checkbox"/>	Ingress ▼
6	<input type="checkbox"/>	Ingress ▼
7	<input type="checkbox"/>	Ingress ▼
24	<input type="checkbox"/>	Ingress ▼
25	<input type="checkbox"/>	Ingress ▼
26	<input type="checkbox"/>	Ingress ▼

Apply Cancel

The following table describes the labels in this screen.

**Table 71** Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Enter the port number of the monitor port.
Egress VLAN	Enter the VLAN ID that the Switch adds to the mirrored traffic before forwarding it out. This allows you to separate the mirrored traffic from the non-mirrored traffic on the monitor port.  The tag will be added even the mirrored traffic is double-tagged.
Port	This field displays the port number.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  <b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are <b>Egress</b> (outgoing), <b>Ingress</b> (incoming) and <b>Both</b> .
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields.

# Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

## 17.1 Link Aggregation Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See [Section 17.6 on page 184](#) for a static port trunking example.

## 17.2 Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The Switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregation Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

## 17.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information<sup>2</sup>:

**Table 72** Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

**Table 73** Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

## 17.3 Link Aggregation Status

Click **Advanced Application > Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See [Section 17.1 on page 180](#) for more information.

**Figure 107** Advanced Application > Link Aggregation Status

Index	Enabled Ports	Synchronized Ports	Aggregator ID	Status
1	-	-	-	-

The following table describes the labels in this screen.

**Table 74** Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Port	These are the ports you have configured in the <b>Link Aggregation</b> screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to <a href="#">Section 17.2.1 on page 181</a> for more information on this field.
Status	This field displays how these ports were added to the trunk group. It displays: <ul style="list-style-type: none"> <li><b>Static</b> - if the ports are configured as static members of a trunk group.</li> <li><b>LACP</b> - if the ports are configured to join a trunk group via LACP.</li> </ul>

2. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

## 17.4 Link Aggregation Setting

Click **Advanced Application > Link Aggregation > Link Aggregation Setting** to display the screen shown next. See [Section 17.1 on page 180](#) for more information on link aggregation.

**Figure 108** Advanced Application > Link Aggregation > Link Aggregation Setting

The following table describes the labels in this screen.

**Table 75** Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Port Selection criteria	Specify the way to choose a port in the trunk group (multiple ports) to transmit/receive packets for different type of traffic. Select one of the following criteria for the port selection.  <b>Source MAC Address:</b> Uses packets' source MAC address as the criteria. <b>Destination MAC Address:</b> Uses packets' destination MAC address as the criteria. <b>Source+Destination MAC Address:</b> Uses packets' both source and destination MAC address as the criteria. <b>Source IP Address:</b> Uses packets' source IP address as the criteria. This can be only used for IPv4 packets. <b>Destination IP Address:</b> Uses packets' destination IP address as the criteria. This can be only used for IPv4 packets. <b>Source+Destination IP Address:</b> Uses packets' both source and destination IP address as the criteria.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs.

**Table 75** Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 17.5 Link Aggregation Control Protocol

Click **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP** to display the screen shown next. See [Section 17.2 on page 180](#) for more information on dynamic link aggregation.

Note: Do not configure this screen unless you want to enable dynamic link aggregation.

**Figure 109** Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

The following table describes the labels in this screen.

**Table 76** Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.

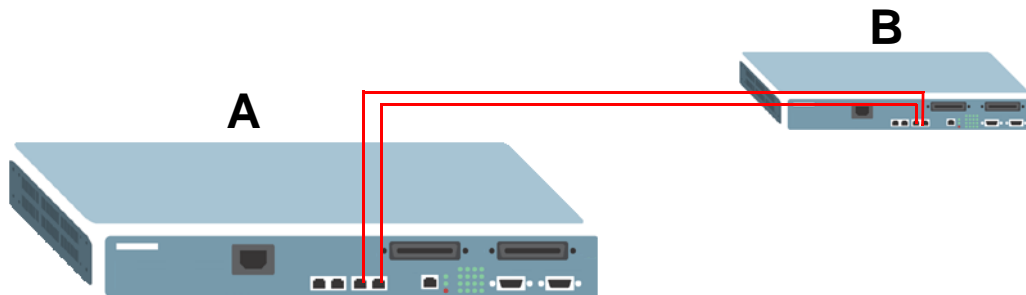
**Table 76** Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  <b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible.  Select either 1 second or 30 seconds.
Apply	Click <b>Apply</b> to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 17.6 Static Trunking Example

This example shows you how to create a static port trunk group for ports 25-26.

- 1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 25-26 on switch **A** connected to switch **B**.

**Figure 110** Trunking Example - Physical Connections



- 2 **Configure static trunking**-Click **Advanced Application > Link Aggregation > Link Aggregation Setting**. In this screen activate trunking group **T1** and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

**Figure 111** Trunking Example - Configuration Screen

The screenshot shows the 'Link Aggregation Setting' configuration screen. At the top right, the status is 'LACP'. Under 'Port Selection criteria', the following options are listed:

- Source MAC Address
- Destination MAC Address
- Source+Destination MAC Address
- Source IP Address
- Destination IP Address
- Source+Destination IP Address

Below this is a table for Group ID and Active status:

Group ID	Active
T1	<input checked="" type="checkbox"/>

Below that is a table for Port and Group assignment:

Port	Group
25	T1
26	T1

At the bottom, there are 'Apply' and 'Cancel' buttons.

Your trunk group 1 (**T1**) configuration is now complete; you do not need to go to any additional screens.

# Port Authentication

This chapter describes the IEEE 802.1x and MAC authentication methods.

## 18.1 Port Authentication Overview

Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports the following methods for port authentication:

- **IEEE 802.1x<sup>3</sup>** - An authentication server validates access to a port based on a username and password provided by the user.
- **MAC** - An authentication server validates access to a port based on the MAC address and password of the client.

Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See [Section 25.1.2 on page 237](#) for more information on configuring your RADIUS server settings.

Note: If you enable IEEE 802.1x authentication and MAC authentication on the same port, the Switch performs IEEE 802.1x authentication first. If a user fails to authenticate via the IEEE 802.1x method, then access to the port is denied.

### 18.1.1 IEEE 802.1x Authentication

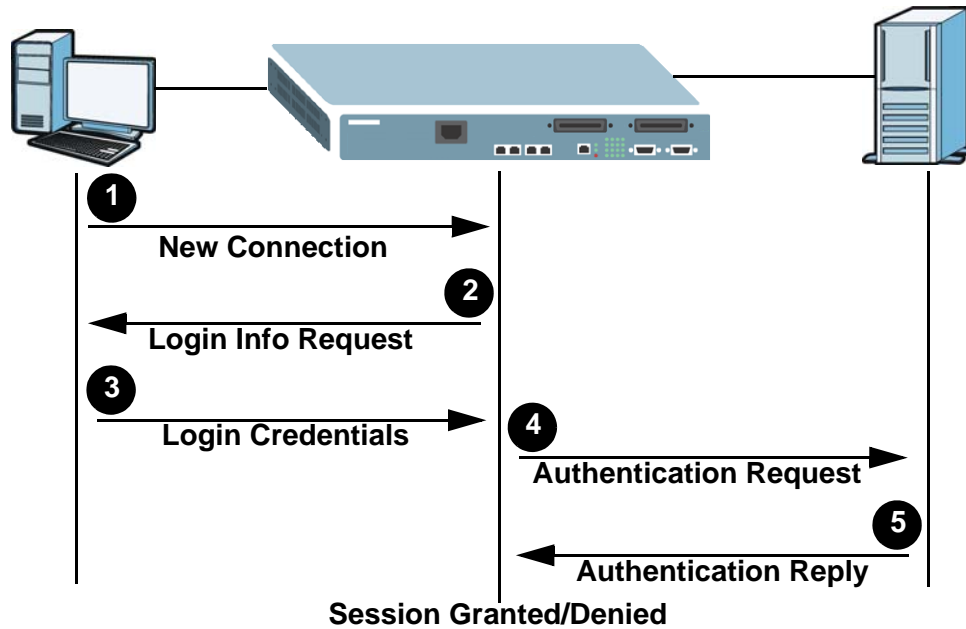
The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an

---

3. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

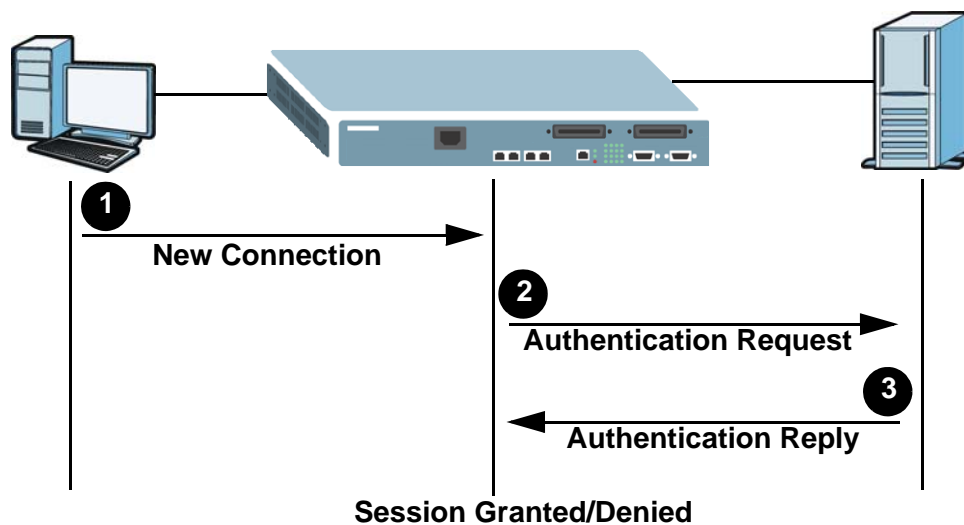
**Figure 112** IEEE 802.1x Authentication Process



## 18.1.2 MAC Authentication

MAC authentication works in a very similar way to IEEE 802.1x authentication. The main difference is that the Switch does not prompt the client for login credentials. The login credentials are based on the source MAC address of the client connecting to a port on the Switch along with a password configured specifically for MAC authentication on the Switch.

**Figure 113** MAC Authentication Process



## 18.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication method(s) you want to use (both on the Switch and the port(s)) then configure the RADIUS server settings in the **Advanced Application > Auth setup > Radius Server Setup** screen.

Click **Advanced Application > Port Authentication** in the navigation panel to display the screen as shown.

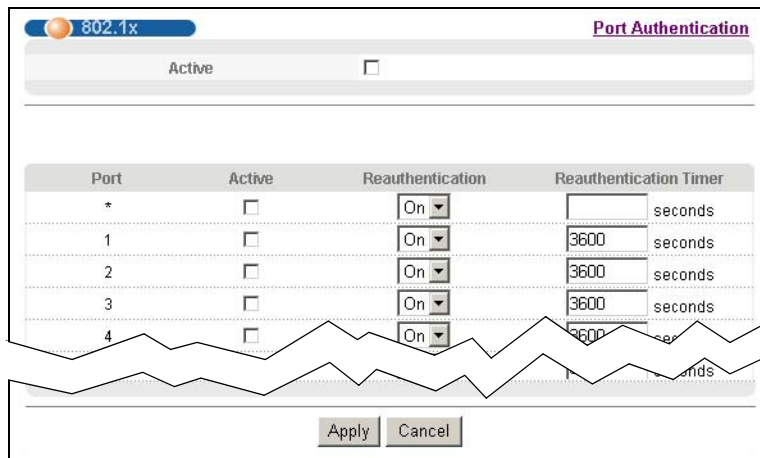
**Figure 114** Advanced Application > Port Authentication



### 18.2.1 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. In the **Port Authentication** screen click **802.1x** to display the configuration screen as shown.

**Figure 115** Advanced Application > Port Authentication > 802.1x



The following table describes the labels in this screen.

**Table 77** Advanced Application > Port Authentication > 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch.  Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays the port number.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.

**Table 77** Advanced Application > Port Authentication > 802.1x (continued)

LABEL	DESCRIPTION
Active	Select this to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 18.2.2 Activate MAC Authentication

Use this screen to activate MAC authentication. In the **Port Authentication** screen click **MAC Authentication** to display the configuration screen as shown.

**Figure 116** Advanced Application > Port Authentication > MAC Authentication

The following table describes the labels in this screen.

**Table 78** Advanced Application > Port Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	Select this check box to permit MAC authentication on the Switch.  Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters.  If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.

**Table 78** Advanced Application > Port Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
Timeout	<p>Specify the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds.</p> <p>When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, then this entry will not be deleted from the MAC address table.</p> <p>Note: If the <b>Aging Time</b> in the <b>Switch Setup</b> screen is set to a lower value, then it supersedes this setting. See <a href="#">Section 8.5 on page 75</a>.</p>
Port	This field displays the port number.
*	<p>Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	Select this to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## MAC Limit

This chapter shows you how to set up port or vlan security by limiting learned MAC addresses.

### 19.1 MAC Limit Overview

MAC limit allows only packets from a limited number of dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port or a VLAN network on the Switch. The Switch can learn up to 16K (16384) MAC addresses in total with no limit on individual ports.

For maximum port security, enable either port security or VLAN security, disable MAC address learning and configure static MAC address(es) for a port or a VLAN.

### 19.2 MAC Limit

Click **Advanced Application** and **MAC Limit** in the navigation panel to display the screen as shown.

**Note:** For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended to disable both **Port Security** and MAC address learning as this will result in many broadcasts.

Figure 117 Advanced Application > MAC Limit

Port	Active SLF drop	MAC Spoofing	Address Learning	Limited Number of Learnt MAC Address
*	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
26	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

The following table describes the labels in this screen.

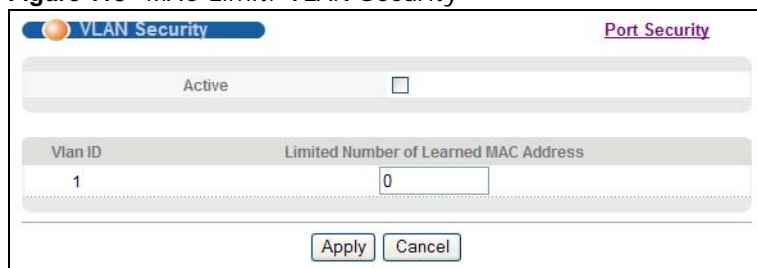
**Table 79** MAC Limit

LABEL	DESCRIPTION
Active	Select this check box to enable the MAC limit feature on the Switch. Clear the check box to disable the feature. You must enable this for the Switch to apply the MAC limit settings for individual ports.
Port	This field displays the number of the port. Use the * entry to configure settings for all of the subscriber ports.
Active SLF drop	SLF stands for Source MAC address Look up Fail (SLF), which means the source MAC does not exist on the Switch. Select this check box to enable the MAC limit feature on this port. The Switch only forwards packets whose source MAC addresses can be found in the MAC address table and drops the other packets. Clear this check box to have the Switch also forward the packets whose source MAC addresses do not exist in the MAC address table.
MAC Spoofing	Select this check box to have the Switch detect whether a MAC address is connected to more than one port. When the Switch detects a spoofed MAC address on a subscriber port, it drops all the packets from the MAC address.
Address Learning	MAC address learning reduces outgoing broadcast traffic. Select this to have the Switch dynamically learn MAC addresses on the port.
Limited Number of Learnt MAC Address	Specify how many MAC addresses the Switch can dynamically learn on this port. For example, if you set this field to "5" on port 2, then only the devices with the first five learned MAC addresses can access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging time can be set in the <b>Basic Setting &gt; Switch Setup</b> screen. The valid range is from 0 to 16K (16384). "0" means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.

### 19.2.1 MAC Limit: VLAN Security

Click the **VLAN Security** link in the **Advanced Application > MAC Limit** screen to display VLAN security settings as the following screen. Use this screen to limit how many MAC addresses the Switch can dynamically learn on individual VLANs.

**Figure 118** MAC Limit: VLAN Security



The following table describes the labels in this screen.

**Table 80** MAC Limit: VLAN Security

LABEL	DESCRIPTION
Active	Select this to limit the number of MAC addresses the Switch can dynamically learn on individual VLANs.



**Table 80** MAC Limit: VLAN Security (continued)

LABEL	DESCRIPTION
Vlan ID	This field displays available VLAN IDs configured in this Switch.
Limited Number of Learned MAC Address	<p>Specify how many MAC addresses the Switch can dynamically learn on this VLAN. For example, if you set this field to "5" on VLAN 2, then only the devices with the first five learned MAC addresses can access VLAN 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging time can be set in the <b>Basic Setting &gt; Switch Setup</b> screen.</p> <p>The valid range is from 0 to 16K (16384 bytes). "0" means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.</p>

# Classifier

This chapter introduces and shows you how to configure the packet classifier on the Switch.

## 20.1 About the Classifier and QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed on a classified traffic flow (refer to [Chapter 21 on page 200](#) to configure policy rules).

## 20.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to [Chapter 21 on page 200](#).

Click **Advanced Application > Classifier** in the navigation panel to display the configuration screen as shown.

**Figure 119** Advanced Application > Classifier

The screenshot shows the 'Classifier' configuration interface. It features a title bar with a logo and the word 'Classifier'. Below this is an 'Active' checkbox. The main area is divided into two sections: 'Layer 2' and 'Layer 3'.  
 In the 'Layer 2' section, there is a 'Name' text field, a 'Packet Format' dropdown menu set to 'All', and several radio button options: 'VLAN' (Any), 'Priority' (0), 'Ethernet Type' (All), 'Source' (MAC Address, Port), and 'Destination' (MAC Address).  
 In the 'Layer 3' section, there are radio button options for 'DSCP' (Any), 'IP Protocol' (All), and 'IP Type' (IPv6). Below these are 'Source' and 'Destination' sections, each with 'IP Address / Address Prefix' text fields and 'Socket Number' radio button options.  
 At the bottom of the form are three buttons: 'Add', 'Cancel', and 'Clear'.

The following table describes the labels in this screen.

**Table 81** Advanced Application > Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are <b>All</b> , <b>802.3 tagged</b> , <b>802.3 untagged</b> , <b>Ethernet II tagged</b> and <b>Ethernet II untagged</b> . A value of <b>802.3</b> indicates that the packets are formatted according to the IEEE 802.3 standards. A value of <b>Ethernet II</b> indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.

**Table 81** Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
Layer 2	
Specify the fields below to configure a layer 2 classifier.	
VLAN	Select <b>Any</b> to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select <b>Any</b> to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select <b>Other</b> and enter the Ethernet type number in hexadecimal value. Refer to <a href="#">Table 83 on page 198</a> for information.
Source	
MAC Address	Select <b>Any</b> to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs). This field is not configurable if you set <b>IP Type</b> to <b>IPv6</b> .
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports ( <b>Any</b> ).
Destination	
MAC Address	Select <b>Any</b> to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs). This field is not configurable if you set <b>IP Type</b> to <b>IPv6</b> .
Layer 3	
Specify the fields below to configure a layer 3 classifier.	
DSCP	Select <b>Any</b> to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select <b>Other</b> and enter the protocol number in decimal value. Refer to <a href="#">Table 84 on page 198</a> for more information.  You may select <b>Establish Only</b> for <b>TCP</b> protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.  The <b>Establish Only</b> option is not selectable if you set <b>IP Type</b> to <b>IPv6</b> .
IP Type	Select to configure an IPv4 or IPv6 address.
Source	
IP Address/Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask. An IPv4 subnet mask can be represented in a 32-bit notation. For example, the subnet mask "255.255.255.0" can be represented as "11111111.11111111.11111111.00000000", and counting up the number of ones in this case results in 24.
Socket Number	<b>Note:</b> You must select either <b>UDP</b> or <b>TCP</b> in the <b>IP Protocol</b> field before you configure the socket numbers.  Select <b>Any</b> to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to <a href="#">Table 85 on page 198</a> for more information.
Destination	

**Table 81** Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
IP Address/Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	<b>Note:</b> You must select either <b>UDP</b> or <b>TCP</b> in the <b>IP Protocol</b> field before you configure the socket numbers.  Select <b>Any</b> to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to <a href="#">Table 85 on page 198</a> for more information.
Add	Click <b>Add</b> to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields back to your previous configuration.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.

## 20.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

**Note:** When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

**Figure 120** Advanced Application > Classifier: Summary Table

Index	Active	Name	Rule	Delete
1	Yes	Example	EtherType = IP; SrcMac = 00:50:ba:ad:4f:81; SrcPort = port 2;	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

**Table 82** Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays <b>Yes</b> when the rule is activated and <b>No</b> when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

**Table 83** Common Ethernet Types and Protocol Numbers

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In the Internet Protocol there is a field, called “Protocol”, to identify the next level protocol. The following table shows some common protocol types and the corresponding protocol number. Refer to <http://www.iana.org/assignments/protocol-numbers> for a complete list.

**Table 84** Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

Some of the most common TCP and UDP port numbers are:

**Table 85** Common TCP and UDP Port Numbers

PROTOCOL NAME	TCP/UDP PORT NUMBER
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110

See [Appendix A on page 397](#) for information on commonly used port numbers.

## 20.4 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

**Figure 121** Classifier: Example

The screenshot displays the 'Classifier' configuration interface. The 'Active' checkbox is checked. The 'Name' field is set to 'Example'. The 'Packet Format' is set to 'All'. Under 'Layer 2', the 'Source' section is highlighted with a red oval, showing 'MAC Address' set to 'Any' and 'Port' set to '2'. The 'Destination' section is also highlighted with a red oval, showing 'MAC Address' set to 'Any'. Under 'Layer 3', the 'IP Type' section is highlighted with a red oval, showing 'IPv4' selected. The 'Source' and 'Destination' sections for Layer 3 are also visible, with 'IP Address / Address Prefix' set to '0.0.0.0' and 'Socket Number' set to 'Any'. At the bottom, there are 'Add', 'Cancel', and 'Clear' buttons.

## Policy Rule

This chapter shows you how to configure policy rules.

### 21.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 20 on page 194](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

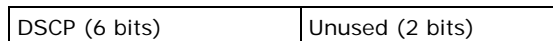
#### 21.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

#### 21.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

### 21.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to [Section 20.2 on page 194](#) for more information.



Click **Advanced Application > Policy Rule** in the navigation panel to display the screen as shown.

**Figure 122** Advanced Application > Policy Rule

Policy																					
Active	<input type="checkbox"/>																				
Name	<input type="text"/>																				
Classifier(s)	PING-VDSL-02																				
Parameters	<table border="0"> <tr> <td>VLAN ID</td> <td><input type="text"/></td> <td>Bandwidth</td> <td><input type="text"/> Kbps</td> </tr> <tr> <td>Egress Port</td> <td><input type="text" value="1"/></td> <td>Out-of-Profile DSCP</td> <td><input type="text"/></td> </tr> <tr> <td>Priority</td> <td><input type="text" value="0"/></td> <td></td> <td></td> </tr> <tr> <td>DSCP</td> <td><input type="text"/></td> <td></td> <td></td> </tr> <tr> <td>TOS</td> <td><input type="text" value="0"/></td> <td></td> <td></td> </tr> </table>	VLAN ID	<input type="text"/>	Bandwidth	<input type="text"/> Kbps	Egress Port	<input type="text" value="1"/>	Out-of-Profile DSCP	<input type="text"/>	Priority	<input type="text" value="0"/>			DSCP	<input type="text"/>			TOS	<input type="text" value="0"/>		
	VLAN ID	<input type="text"/>	Bandwidth	<input type="text"/> Kbps																	
	Egress Port	<input type="text" value="1"/>	Out-of-Profile DSCP	<input type="text"/>																	
	Priority	<input type="text" value="0"/>																			
	DSCP	<input type="text"/>																			
	TOS	<input type="text" value="0"/>																			
Action	<b>Forwarding</b> <input checked="" type="radio"/> No change <input type="radio"/> Discard the packet <input type="radio"/> Do not drop the matching frame previously marked for dropping																				
	<b>Priority</b> <input checked="" type="radio"/> No change <input type="radio"/> Set the packet's 802.1 priority <input type="radio"/> Send the packet to priority queue <input type="radio"/> Replace the 802.1 priority field with the IP TOS value																				
	<b>Diffserv</b> <input checked="" type="radio"/> No change <input type="radio"/> Set the packet's TOS field <input type="radio"/> Replace the IP TOS field with the 802.1 priority value <input type="radio"/> Set the Diffserv Codepoint field in the frame																				
	<b>Outgoing</b> <input type="checkbox"/> Send the packet to the mirror port <input type="checkbox"/> Send the packet to the egress port <input type="checkbox"/> Set the packet's VLAN ID																				
	<b>Metering</b> <input type="checkbox"/> Enable																				
	<b>Out-of-profile action</b> <input type="checkbox"/> Drop the packet <input type="checkbox"/> Change the DSCP value <input type="checkbox"/> Set Out-Drop Precedence <input type="checkbox"/> Do not drop the matching frame previously marked for dropping																				
	<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>																				
	<table border="1"> <thead> <tr> <th>Index</th> <th>Active</th> <th>Name</th> <th>Classifier(s)</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;"> <input type="button" value="Delete"/> <input type="button" value="Cancel"/> </td> </tr> </tbody> </table>		Index	Active	Name	Classifier(s)	Delete					<input type="button" value="Delete"/> <input type="button" value="Cancel"/>									
	Index	Active	Name	Classifier(s)	Delete																
					<input type="button" value="Delete"/> <input type="button" value="Cancel"/>																

The following table describes the labels in this screen.

**Table 86** Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the <b>Classifier</b> screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters	
Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the <b>Action</b> field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 1 and 1000000.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action	
Specify the action(s) the Switch takes on the associated classified traffic flow.	
Forwarding	Select <b>No change</b> to forward the packets. Select <b>Discard the packet</b> to drop the packets. Select <b>Do not drop the matching frame previously marked for dropping</b> to retain the frames that were marked to be dropped before.
Priority	Select <b>No change</b> to keep the priority setting of the frames. Select <b>Set the packet's 802.1 priority</b> to replace the packet's 802.1 priority field with the value you set in the <b>Priority</b> field. Select <b>Send the packet to priority queue</b> to put the packets in the designated queue. Select <b>Replace the 802.1 priority field with the IP TOS value</b> to replace the packet's 802.1 priority field with the value you set in the <b>TOS</b> field.
Diffserv	Select <b>No change</b> to keep the TOS and/or DSCP fields in the packets. Select <b>Set the packet's TOS field</b> to set the TOS field with the value you configure in the <b>TOS</b> field. Select <b>Replace the IP TOS with the 802.1 priority value</b> to replace the TOS field with the value you configure in the <b>Priority</b> field. Select <b>Set the Diffserv Codepoint field in the frame</b> to set the DSCP field with the value you configure in the <b>DSCP</b> field.

**Table 86** Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Outgoing	<p>Select <b>Send the packet to the mirror port</b> to send the packet to the mirror port.</p> <p>Select <b>Send the packet to the egress port</b> to send the packet to the egress port.</p> <p>Select <b>Set the packet's VLAN ID</b> to add a VLAN ID to the matched packet or replace the VLAN ID of the packets with the value you configure in the <b>VLAN ID</b> field.</p>
Metering	<p>Select <b>Enable</b> to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.</p>
Out-of-profile action	<p>Select the action(s) to be performed for out-of-profile traffic.</p> <p>Select <b>Drop the packet</b> to discard the out-of-profile traffic.</p> <p>Select <b>Change the DSCP value</b> to replace the DSCP field with the value specified in the <b>Out of profile DSCP</b> field.</p> <p>Select <b>Set Out-Drop Precedence</b> to mark out-of-profile traffic and drop it when network is congested.</p> <p>Select <b>Do not drop the matching frame previously marked for dropping</b> to queue the frames that are marked to be dropped.</p>
Add	<p>Click <b>Add</b> to inset the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click <b>Cancel</b> to reset the fields back to your previous configuration.</p>
Clear	<p>Click <b>Clear</b> to set the above fields back to the factory defaults.</p>
Index	<p>This field displays the policy index number. Click an index number to edit the policy.</p>
Active	<p>This field displays <b>Yes</b> when policy is activated and <b>No</b> when is it deactivated.</p>
Name	<p>This field displays the name you have assigned to this policy.</p>
Classifier(s)	<p>This field displays the name(s) of the classifier to which this policy applies.</p>
Delete	<p>Click <b>Delete</b> to remove the selected entry from the summary table.</p>
Cancel	<p>Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.</p>

## 21.3 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to [Section 20.4 on page 199](#)).

**Figure 123** Policy Example

The screenshot displays the 'Policy' configuration interface. The 'Name' field is set to 'Test'. The 'Classifier(s)' dropdown menu is open, showing 'PING-VDSL-03' and 'Example' (selected). The 'Parameters' section includes 'VLAN ID', 'Egress Port' (set to 1), 'Priority' (0), 'DSCP', and 'TOS' (0). The 'Metering' section shows 'Bandwidth' set to 10000 Kbps and 'Out-of-Profile DSCP' set to an empty field. The 'Action' section includes 'Forwarding' (No change selected), 'Priority' (No change selected), 'Diffserv' (No change selected), 'Outgoing' (Send the packet to the mirror port, Send the packet to the egress port, Set the packet's VLAN ID), and 'Metering' (Enable selected, Drop the packet selected). The 'Out-of-profile action' section includes 'Change the DSCP value', 'Set Out-Drop Precedence', and 'Do not drop the matching frame previously marked for dropping'. The 'Add', 'Cancel', and 'Clear' buttons are at the bottom.

# Queuing Method

This chapter introduces the queuing methods supported.

## 22.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

### 22.1.1 Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

### 22.1.2 Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (portion) (the number you configure in the Weight field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on. Guaranteed quantum is calculated as Queue Weight x 2048 bytes.

### 22.1.3 Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with

smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

## 22.2 Configuring Queuing

Click **Advanced Application > Queuing Method** in the navigation panel.

**Figure 124** Advanced Application > Queuing Method

**Queuing Method**

Method

SPQ  
 WFQ  
 WRR

VDSL Port SPQ Enable: None

Port	Weight								GE Port SPQ Enable	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
*										None
1	1	2	3	4	5	6	7	8		-
2	1	2	3	4	5	6	7	8		-
3	1	2	3	4	5	6	7	8		-
4	1	2	3	4	5	6	7	8		-
5	1	2	3	4	5	6	7	8		-
6	1	2	3	4	5	6	7	8		-
25	1	2	3	4	5	6	7	8		None
26	1	2	3	4	5	6	7	8		None

Apply Cancel

The following table describes the labels in this screen.

**Table 87** Advanced Application > Queuing Method

LABEL	DESCRIPTION
Method	<p>Select <b>SPQ</b> (Strictly Priority Queuing), <b>WFQ</b> (Weighted Fair Queuing) or <b>WRR</b> (Weighted Round Robin).</p> <p>Strictly Priority services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest.</p> <p>Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the <b>Weight</b> field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights.</p> <p>Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue <b>Weight</b> field). Queues with larger weights get more service than queues with smaller weights.</p>
VDSL Port SPQ Enable	<p>This field is applicable only when you select <b>WFQ</b> or <b>WRR</b>.</p> <p>Select a queue (<b>Q0</b> to <b>Q7</b>) to have the Switch use <b>SPQ</b> to service the subsequent queue(s) after and including the specified queue for the VDSL ports. For example, if you select <b>Q5</b>, the Switch services traffic on <b>Q5</b>, <b>Q6</b> and <b>Q7</b> using <b>SPQ</b>.</p> <p>Select <b>None</b> to always use <b>WFQ</b> or <b>WRR</b> for the VDSL ports.</p>
Port	<p>This label shows the port you are configuring.</p>
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p><b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.</p>
Weight	<p>When you select <b>WFQ</b> or <b>WRR</b> enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.</p>
GE Port SPQ Enable	<p>This field is applicable only when you select <b>WFQ</b> or <b>WRR</b>.</p> <p>Select a queue (<b>Q0</b> to <b>Q7</b>) to have the Switch use <b>SPQ</b> to service the subsequent queue(s) after and including the specified queue for the gigabit ports. For example, if you select <b>Q5</b>, the Switch services traffic on <b>Q5</b>, <b>Q6</b> and <b>Q7</b> using <b>SPQ</b>.</p> <p>Select <b>None</b> to always use <b>WFQ</b> or <b>WRR</b> for the gigabit ports.</p>
Apply	<p>Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click <b>Cancel</b> to begin configuring this screen afresh.</p>

# VLAN Stacking

This chapter shows you how to configure VLAN stacking on your Switch. See the chapter on VLANs for more background information on Virtual LAN.

## 23.1 VLAN Stacking Overview

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

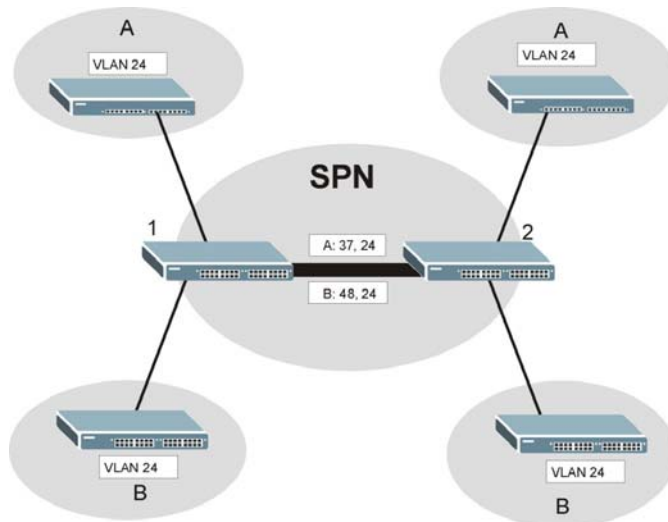
### 23.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by



adding tag 37 to distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

**Figure 125** VLAN Stacking Example



## 23.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel** (the latter is for Gigabit ports only).

Note: Some devices do not support all roles.

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as “untagged”, so a second VLAN tag (outer VLAN tag) can be added.

Note: Static VLAN **Tx Tagging** MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

Note: Static VLAN **Tx Tagging** MUST be enabled on a port where you choose **Tunnel Port**.

## 23.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

**Table 88** VLAN Tag Format

TPID	Priority	VID
------	----------	-----

**TPID** (Tag Protocol Identifier) is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. The value of this field is 0x8100 as defined in IEEE 802.1Q. Other vendors may use a different value, such as 0x9100.

**Tunnel TPID** is the VLAN stacking tag type the Switch adds to the outgoing frames sent through a **Tunnel Port** of the service provider's edge devices (1 and 2 in the VLAN stacking example figure).

**Priority** refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the Switch, configure priority level of inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

**VID** is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

### 23.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the Switch **VLAN Stacking** screen.

**Table 89** Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	<b>TPID</b>	<b>Priority</b>	<b>VID</b>	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	<b>Tunnel TPID</b>	<b>Priority</b>	<b>VID</b>	<b>TPID</b>	<b>Priority</b>	<b>VID</b>	Len/Etype	Data	FCS	Double-tagged frame

**Table 90** 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
Tunnel TPID	Tag Protocol Identifier added on a tunnel port	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

## 23.4 Configuring VLAN Stacking

Click **Advanced Application > VLAN Stacking** to display the screen as shown.

Note: You can not enable VLAN mapping and VLAN stacking at the same time.

**Figure 126** Advanced Application > VLAN Stacking

Port	Role	Tunnel TPID
*	Normal	
1	Normal	8100
2	Normal	8100
3	Normal	8100
4	Normal	8100
5	Normal	8100
6	Normal	8100
7	Normal	8100
8	Normal	8100
9	Normal	8100
10	Normal	8100
11	Normal	8100
12	Normal	8100
13	Normal	8100
14	Normal	8100
15	Normal	8100
16	Normal	8100
17	Normal	8100
18	Normal	8100
19	Normal	8100
20	Normal	8100
21	Normal	8100
22	Normal	8100
23	Normal	8100
24	Normal	8100
25	Normal	8100
26	Normal	8100

The following table describes the labels in this screen.

**Table 91** Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Active	Select this to enable VLAN stacking on the Switch.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.

**Table 91** Advanced Application > VLAN Stacking (continued)

LABEL	DESCRIPTION
Role	<p>Select <b>Normal</b> to have the Switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in <b>SPVID</b> and <b>Priority</b> of the <b>Port-based QinQ</b> or the <b>Selective QinQ</b> screen are ignored.</p> <p>Select <b>Access Port</b> for ingress ports at the edge of the service provider's network.</p> <p>Select <b>Tunnel Port</b> (available for Gigabit ports only) for egress ports at the edge of the service provider's network. Select <b>Tunnel Port</b> to have the Switch add the <b>Tunnel TPID</b> tag to all outgoing frames sent on this port.</p> <p>In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.</p>
Tunnel TPID	<p>TPID is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Enter a four-digit hexadecimal number from 0000 to FFFF that the Switch adds in the outer VLAN tag of the frames sent on the tunnel port(s). The Switch also uses this to check if the received frames are double-tagged.</p> <p>The value of this field is 0x8100 as defined in IEEE 802.1Q. If the Switch needs to communicate with other vendors' devices, they should use the same TPID.</p> <p><b>Note:</b> You can define up to four different tunnel TPIDs (including <b>8100</b>) in this screen at a time.</p>
Apply	<p>Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click <b>Cancel</b> to begin configuring this screen afresh.</p>

### 23.4.1 Port-based Q-in-Q

Port-based Q-in-Q lets the Switch treat all frames received on the same port as the same VLAN flows and add the same outer VLAN tag to them, even they have different customer VLAN IDs.

Click **Port-based QinQ** in the **Advanced Application > VLAN Stacking** screen to display the screen as shown.

**Figure 127** VLAN Stacking > Port-based QinQ

Port	SPVID	Copy Ctag Priority	Priority
*	<input type="text"/>	<input type="checkbox"/>	0 ▼
1	1	<input type="checkbox"/>	0 ▼
2	1	<input type="checkbox"/>	0 ▼
3	1	<input type="checkbox"/>	0 ▼
4	1	<input type="checkbox"/>	0 ▼
5	1	<input type="checkbox"/>	0 ▼
6	1	<input type="checkbox"/>	0 ▼
7	1	<input type="checkbox"/>	0 ▼
8	1	<input type="checkbox"/>	0 ▼
9	1	<input type="checkbox"/>	0 ▼
25	1	<input type="checkbox"/>	0 ▼
26	1	<input type="checkbox"/>	0 ▼

The following table describes the labels in this screen.

**Table 92** VLAN Stacking > Port-based QinQ

LABEL	DESCRIPTION
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  <b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.
SPVID	<b>SPVID</b> is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See <a href="#">Chapter 10 on page 129</a> for more background information on VLAN ID.
Copy Ctag Priority	Select the checkbox to set the priority in the service provider (outer) VLAN tag to be the same as the priority in the customer (inner) VLAN tag for the frames received on this port.
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. This field is not applicable if the <b>Copy Ctag Priority</b> checkbox is selected.  "0" is the lowest priority level and "7" is the highest.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.4.2 Selective Q-in-Q

Selective Q-in-Q is VLAN-based. It allows the Switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags.

Note: Selective Q-in-Q rules are only applied to single-tagged frames received on the access ports. If the incoming frames are untagged or single-tagged but received on a tunnel port or cannot match any selective Q-in-Q rules, the Switch applies the port-based Q-in-Q rules to them.

Click **Selective QinQ** in the **Advanced Application > VLAN Stacking** screen to display the screen as shown.

**Figure 128** VLAN Stacking > Selective QinQ

The following table describes the labels in this screen.

**Table 93** VLAN Stacking > Selective QinQ

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	The port number identifies the port you are configuring.
CVID	Enter a customer VLAN ID (the inner VLAN tag) from 1 to 4094. This is the VLAN tag carried in the packets from the subscribers.
SPVID	<b>SPVID</b> is the service provider’s VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See <a href="#">Chapter 10 on page 129</a> for more background information on VLAN ID.
Priority	Select the <b>Active</b> checkbox and a priority level (from 0 to 7). This is the service provider’s priority level that adds to the frames received on this port. If you clear the <b>Active</b> checkbox, the SPVID priority will be 0.  "0" is the lowest priority level and "7" is the highest.
Add	Click <b>Add</b> to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Index	This is the number of the selective VLAN stacking rule.

**Table 93** VLAN Stacking > Selective QinQ (continued)

LABEL	DESCRIPTION
Active	This shows whether this rule is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied.
CVID	This is the customer VLAN ID in the incoming packets.
SPVID	This is the service provider's VLAN ID that adds to the packets from the subscribers.
Priority	This is the service provider's priority level in the packets.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.

### 23.4.3 Port-based InnerQ

Port-based InnerQ allows you to add a customer VLAN (the inner tag) tag to untagged incoming frames before adding the service provider's VLAN tag (the outer tag) and forwarding them out. This feature is not applicable on a tunnel port.

Click **Port-based InnerQ** in the **Advanced Application > VLAN Stacking** screen to display the screen as shown.

**Figure 129** VLAN Stacking > Port-based InnerQ

The screenshot shows the 'Port-based InnerQ' configuration interface. At the top, there is a blue header with a gear icon and the text 'Port-based InnerQ'. To the right, there is a link for 'VLAN Stacking'. Below the header is a table with the following columns: 'Port', 'Active', 'CPVID', 'Priority', and 'Remove InnerQ'. The table contains 26 rows, one for each port. The 'Active' column has checkboxes, all of which are currently unchecked. The 'CPVID' column has text input fields, all containing the value '1'. The 'Priority' column has dropdown menus, all set to '0'. The 'Remove InnerQ' column has checkboxes, all of which are currently unchecked. At the bottom of the table, there are two buttons: 'Apply' and 'Cancel'.

Port	Active	CPVID	Priority	Remove InnerQ
*	<input type="checkbox"/>		0	<input type="checkbox"/>
1	<input type="checkbox"/>	1	0	<input type="checkbox"/>
2	<input type="checkbox"/>	1	0	<input type="checkbox"/>
3	<input type="checkbox"/>	1	0	<input type="checkbox"/>
4	<input type="checkbox"/>	1	0	<input type="checkbox"/>
5	<input type="checkbox"/>	1	0	<input type="checkbox"/>
6	<input type="checkbox"/>	1	0	<input type="checkbox"/>
7	<input type="checkbox"/>	1	0	<input type="checkbox"/>
8	<input type="checkbox"/>	1	0	<input type="checkbox"/>
9	<input type="checkbox"/>	1	0	<input type="checkbox"/>
10	<input type="checkbox"/>		0	<input type="checkbox"/>
25	<input type="checkbox"/>	1	0	<input type="checkbox"/>
26	<input type="checkbox"/>	1	0	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 94** VLAN Stacking > Port-based InnerQ

LABEL	DESCRIPTION
Port	The port number identifies the port you are configuring.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Changes in this row are copied to all the ports as soon as you make them.</p>
Active	Check this box to activate this rule.
CPVID	<b>CPVID</b> is the customer port VLAN ID (the inner VLAN tag). Enter the customer VLAN ID (from 1 to 4094) for frames received on this port. See <a href="#">Chapter 10 on page 129</a> for more background information on VLAN ID.
Priority	<p>Select a priority level (from 0 to 7). This is the priority level in the customer VLAN tag that adds to the frames received on this port.</p> <p>"0" is the lowest priority level and "7" is the highest.</p>
Remove InnerQ	<p>Select the check box to remove the customer VLAN tag from outgoing traffic on this port.</p> <p>This feature is not applicable on a tunnel port.</p>
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



This chapter shows you how to configure various multicast features.

## 24.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

### 24.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

### 24.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the Switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

### 24.1.3 IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

## 24.1.4 IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

## 24.1.5 IGMP Proxy

IGMP proxy enables a layer-2 switch to maintain a joined member list for each IGMP group on the switch. This switch automatically and periodically sends queries to the VDSL ports to get the subscribing information and response the upper layer router's query for the member list. In addition, it enables the switch not to report the leave request sent from one subscriber to upper layer router if there are still other subscriber(s) in the same IGMP group. It also allows the switch not to report the join request sent from one subscriber to upper layer router if any subscriber is still in the same IGMP group. In other words, an IGMP proxy switch only forward the first join request and the last leave request in an IGMP network to its upper layer router. It can reduce multicast traffic significantly.

Note: Note: You must set one of Gigabit Ethernet ports to "Fixed mode" before enabling IGMP proxy.

## 24.1.6 Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

## 24.1.7 MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. If the leave mode is not set to immediate, the router or switch sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

## 24.2 Multicast Status

Click **Advanced Application > Multicast** to display the screen as shown. This screen shows the multicast group information. See [Section 24.1 on page 217](#) for more information on multicasting.

**Figure 130** Advanced Application > Multicast Status

**Multicast Status**
**Multicast Setting**

Port	Total	VID	Multicast Group ( Filter Mode ) Source Address	Client IP	Up Time
1 - B02*	1	4001	224.1.4.102 ( EXCLUDE )	10.173.92.174	0:51:08
3	1	4001	224.1.4.84 ( EXCLUDE )	10.173.92.133	0:51:08
7	1	4001	230.1.2.165 ( EXCLUDE )	10.173.92.137	0:53:55
9 - B03*	1	4001	224.1.4.30 ( EXCLUDE )	10.173.92.108	0:51:07
23 - B12*	1	4001	224.1.4.89 ( EXCLUDE )	10.173.92.161	0:51:08

**Multicast Group Member**

VID	Total	Multicast Group	Number	Member
4001	11	224.1.4.30	1	9(B3)
		224.1.4.54	1	14
		224.1.4.84	1	3
		224.1.4.89	2	23(B12),15
		224.1.4.95	1	19
		224.1.4.102	1	1(B2)
		230.1.2.165	2	7,13
		230.1.2.226	1	11(B4)
		230.1.2.227	1	22

**Clear IGMP Counter**

Any Port ▼
 Port 1 - B02\* ▼

**IGMP Per Port Receive Counter**

Port	Report In			Query In			Dropped By	
	V1	V2	Leave	V1	V2	V3	Rate	Others
1 - B02*	0	120	0	0	0	0	0	0
3	0	95	0	0	0	0	0	0
4	0	62	0	0	0	0	0	0
5 - B05*	0	0	0	0	0	0	0	38**
26	0	0	0	0	0	0	0	0

**IGMP Per Port Specific Counter**

Port	Total			Dropped By			
	GroupNum	Join	Leave	MaxGroup	Filter	MVR	Others
1 - B02*	1	30	0	0	90	0	0
3	1	32	0	0	63	0	0
4	0	0	0	0	62	0	0
5 - B05*	0	0	0	0	60	0	0
26	0	0	0	0	0	0	0

**IGMP Per Port Transmit Counter**

Port	Report Out			Query Out		
	V1	V2	Leave	V1	V2	V3
1 - B02*	0	0	0	0	40	0
3	0	0	0	0	40	0
4	0	0	0	0	40	0
25	0	350	18	0	0	0
26	0	0	0	0	0	0

IGMP Per VLAN Receive Counter										
VID	V1	V2	Report In			Query In			Dropped By	
			Leave	V3	V1	V2	V3	Rate	Others	
14	0	95	0	0	0	0	0	0	0	
16	0	62	0	0	0	0	0	0	0	
18	0	60	0	0	0	0	0	0	0	
64	0	70	0	0	0	0	0	0	0	
4093	0	0	0	0	0	0	0	0	35	

IGMP Per VLAN Specific Counter							
VID	Total			Dropped By			
	GroupNum	Join	Leave	MaxGroup	Filter	MVR	Others
14	0	0	0	0	63	0	0
16	0	0	0	0	62	0	0
18	0	0	0	0	60	0	0
4001	11	358	11	0	0	0	0
4093	0	0	0	0	0	0	0

IGMP Per VLAN Transmit Counter								
VID	V1	V2	Report Out		Query Out			
			Leave	V3	V1	V2	V3	
14	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	
18	0	0	0	0	0	0	0	
54	0	0	0	0	0	0	0	
4001	0	350	18	0	0	651	0	

IGMP Per Port Querier Source IP			
Index	Port	VID	Querier Source IP
1	25	4001	172.100.24.81

The following table describes the labels in this screen.

**Table 95** Advanced Application > Multicast Status

LABEL	DESCRIPTION
Port	This column displays the numbers of the ports belonging to a multicast group and the port's bonding group ID if it is a member of one. A star (*) displays if the port is the main port in the bonding group.
Total	This field displays to how many multicast groups this port belongs. In the IPTV application, a multicast group represents a TV channel. This field shows how many TV channels have been subscribed to on this port.
VID	This field displays the multicast VLAN ID.
Multicast Group (Filter Mode) Source Address	<p>This field displays the multicast group source address and source filtering mode. In IPTV, the multicast group source address means the address of a media server which provides media content.</p> <p>IGMPv3 and MLDv2 supports multicast source filtering.</p> <p>In <b>INCLUDE</b> mode, the client listens to the specified sources only.</p> <p>In <b>EXCLUDE</b> mode, the client listens to all sources other than the specified address.</p> <p>When the Switch receives a multicast packet destined to a configured multicast group and the packet's source address is in the INCLUDE list or not in the EXCLUDE list, the Switch forwards the packets to the clients that join this group.</p>
Client IP	This field displays an IP address which is a member in this multicast group. In IPTV, this means the IP address of a set-top box connected to this port.

**Table 95** Advanced Application > Multicast Status (continued)

LABEL	DESCRIPTION
Up Time	This field displays how long (in hh:mm:ss format) this port has been a member of the multicast group since the last time it joined. In IPTV, this means how long a user has been watching this channel.
Multicast Group Member	
VID	This field displays the multicast VLAN ID.
Total	This field displays how many ports in this VLAN.
Multicast Group	This field displays the IP multicast group addresses in this VLAN.
Number	This field displays how many ports belong to this multicast group.
Member	This field displays the port number(s) that belong to the multicast group. The port's bonding group ID also displays in brackets if the port has joined one.
Clear IGMP Counter	
Any	Select this, select <b>Port</b> or <b>Vlan</b> from the drop-down list box and then click <b>Clear Counter</b> to have the Switch clear IGMP counters for all ports or for all VLANs.
Port	Select this, select a port number from the drop-down list box and then click <b>Clear Counter</b> to have the Switch clear IGMP counters for the port.
IGMP Per Port Receive Counter	
This section displays incoming multicast traffic statistics per port.	
Port	This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.
Report In	This column displays how many <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast join messages and multicast <b>Leave</b> messages the port has received since the last start up or clearing of the IGMP counters. <b>V1</b> , <b>V2</b> , and <b>V3</b> means IGMP versions 1, 2 and 3.
Query In	This column displays how many <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast queries the port has received.
Dropped By	<p>This column displays the number of multicast queries this port has dropped due to the following reasons:</p> <p><b>Rate:</b> the receiving rate exceeds the configured rate limit setting. You can configure the limit setting for the port in the <b>Basic Setting &gt; Port Setup</b> and <b>Basic Setting &gt; Rate Limit Profile Setup</b> screen.</p> <p><b>Others:</b> packets are dropped due to reasons other than the previous one.</p>
IGMP Per Port Specific Counter	
This section displays multicast traffic statistics per port.	
Port	This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.
Total GroupNum	This field displays the total number of multicast groups this port has learned since the last start up or clearing of the IGMP counters.
Join	This field displays the number of multicast groups in Join messages this port has received.
Leave	This field displays the number of multicast groups in Leave messages this port has received.

**Table 95** Advanced Application > Multicast Status (continued)

LABEL	DESCRIPTION
Dropped By	<p>This column displays the number of multicast queries this port has dropped due to the following reasons:</p> <p><b>MaxGroup:</b> the number of multicast groups the port has joined exceeds the per-port Max Group Limit configured in the <b>Advanced Application &gt; Multicast &gt; Multicast Setting</b> screen.</p> <p><b>Filter:</b> the port is not allowed to join a multicast group in a multicast join message this port received. You can configure the filtering list in the <b>Advanced Application &gt; Multicast &gt; Multicast Setting</b> and <b>Multicast &gt; Multicast Setting &gt; IGMP Filtering Profile</b> screens.</p> <p><b>MVR:</b> this port is not configured as a receiver port in the MVR multicast VLAN. You can configure the MVR settings in the <b>Advanced Application &gt; Multicast &gt; Multicast Setting &gt; MVR</b> screen.</p> <p><b>Others:</b> reasons other than the ones described above, such as the Switch has insufficient memory.</p>
IGMP Per Port Transmit Counter	
This section displays outgoing multicast traffic statistics per port.	
Port	This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.
Report Out	This column displays how many <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast join messages and multicast <b>Leave</b> messages the port has transmitted. <b>V1</b> , <b>V2</b> , and <b>V3</b> means IGMP versions 1, 2 and 3.
Query Out	This column displays how many valid <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast queries the port has transmitted.
IGMP Per VLAN Receive Counter	
This section displays incoming multicast traffic statistics per VLAN network.	
VID	This field displays a multicast VLAN ID.
Report In	This column displays how many <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast join messages and multicast <b>Leave</b> messages this VLAN network has received. <b>V1</b> , <b>V2</b> , and <b>V3</b> means IGMP versions 1, 2 and 3.
Query In	This column displays how many valid <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast queries this VLAN network has received.
Dropped By	<p>This column displays how many multicast queries that have been dropped in this VLAN due to the following reasons:</p> <p><b>Rate:</b> the receiving rate of the ports in this VLAN exceeds the configured rate limits. You can configure the limit settings in the <b>Basic Setting &gt; Port Setup</b> and <b>Basic Setting &gt; Rate Limit Profile Setup</b> screens.</p> <p><b>Others:</b> reasons other than the previous one.</p>
IGMP Per VLAN Specific Counter	
This section displays multicast traffic statistics per VLAN network.	
Total GroupNum	This field displays the total number of multicast groups this VLAN network has learned since the last start up or clearing of the IGMP counters.

**Table 95** Advanced Application > Multicast Status (continued)

LABEL	DESCRIPTION
Dropped By	<p>This column displays how many multicast queries that have been dropped in this VLAN due to the following reasons:</p> <p><b>MaxGroup:</b> the number of multicast groups the ports in this VLAN have joined exceeds the per-port Max Group Limit configured in the <b>Advanced Application &gt; Multicast &gt; Multicast Setting</b> screen.</p> <p><b>Filter:</b> the VLAN is not allowed to join a multicast group in a multicast join message the ports in this VLAN received. You can configure the filtering list in the <b>Advanced Application &gt; Multicast &gt; Multicast Setting</b> and <b>Multicast &gt; Multicast Setting &gt; IGMP Filtering Profile</b> screens.</p> <p><b>MVR:</b> the receiving ports in this VLAN are not the receiver ports in the MVR multicast VLANs. You can configure the MVR settings in the <b>Advanced Application &gt; Multicast &gt; Multicast Setting &gt; MVR</b> screen.</p> <p><b>Others:</b> reasons other than the ones described above, such as the Switch has insufficient memory.</p>
IGMP Per VLAN Transmit Counter	
This section displays outgoing multicast traffic statistics per VLAN network.	
Report Out	This column displays how many <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast join messages and multicast <b>Leave</b> messages sent on a VLAN network. <b>V1</b> , <b>V2</b> , and <b>V3</b> means IGMP versions 1, 2 and 3.
Query Out	This column displays how many valid <b>V1</b> , <b>V2</b> , and <b>V3</b> multicast queries sent on a VLAN network.
IGMP Per Port Querier Source IP	
Index	The index number of an entry in this table.
Port	The number of a port which has received multicast queries.
VID	The VLAN ID to which the received multicast queries belong.
Querier Source IP	The IP address of the device which sent the multicast queries.

## 24.3 Multicast Setting

Click **Advanced Application > Multicast > Multicast Setting** link to display the screen as shown. See [Section 24.1 on page 217](#) for more information on multicasting.

**Figure 131** Advanced Application > Multicast > Multicast Setting

Port	Immed. Leave	Max Group Num.	IGMP Msg Limit	IGMP Filtering Profile	IGMP Querier Mode
*	<input type="checkbox"/>	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	Default	Auto
1	<input type="checkbox"/>	<input type="checkbox"/> Enable 0	<input type="checkbox"/> Enable 0	Default	Edge
2	<input type="checkbox"/>	<input type="checkbox"/> Enable 0	<input type="checkbox"/> Enable 0	Default	Edge
3	<input type="checkbox"/>	<input type="checkbox"/> Enable 0	<input type="checkbox"/> Enable 0	Default	Edge
4	<input type="checkbox"/>	<input type="checkbox"/> Enable 0	<input type="checkbox"/> Enable 0	Default	Edge
26	<input type="checkbox"/>	<input type="checkbox"/> Enable 0	<input type="checkbox"/> Enable 0	Default	Auto

The following table describes the labels in this screen.

**Table 96** Advanced Application > Multicast > Multicast Setting

LABEL	DESCRIPTION
IGMP Action	Use these settings to configure multicast group membership discovery.
Active	Select <b>None</b> to disable multicast group membership discovery on the Switch. Select <b>Snooping</b> to enable IGMP/MLD snooping to forward group multicast traffic only to ports that are members of that group. Select <b>Proxy</b> to enable IGMP/MLD proxy to decrease subscriber's join/leave messages forwarding in a group.
Enable MLD	Enables Multicast Listener Discovery version one (MLD v1) and version two (MLD v2) on the Switch. See <a href="#">Section 24.1.6 on page 218</a> for information about MLD.
Host Timeout	Specify the time (from 1 to 16,711,450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16,711,450) in seconds. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select <b>No-Change</b> to not replace the priority.



**Table 96** Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
IGMP Filtering	<p>Select <b>Active</b> to enable IGMP filtering to control which IGMP groups a subscriber on a port can join.</p> <p>Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.</p>
Proxy	<p>Select <b>MGMDv3 Mode</b> to enable Multicast Group Membership Discovery version three (MGMDv3) and have the Switch send IGMPv3 or MLDv2 queries instead of IGMPv2 or MLDv1 queries.</p> <p>MGMDv2 indicates IGMPv2 in IPv4 networks and MLDv1 in IPv6 networks. MGMDv3 indicates IGMPv3 in IPv4 networks and MLDv2 in IPv6 networks.</p> <p>Note: MGMDv3 only applies in IGMP proxy mode.</p>
Unknown Multicast Frame	<p>Specify the action to perform when the Switch receives an unknown multicast frame. Select <b>Drop</b> to discard the frame(s). Select <b>Flooding</b> to send the frame(s) to all ports.</p>
Reserved Multicast Group	<p>Multicast addresses (224.0.0.0 to 224.0.0.255) are reserved for the local scope. For examples, 224.0.0.1 is for all hosts in this subnet, 224.0.0.2 is for all multicast routers in this subnet, etc. A router will not forward a packet with the destination IP address within this range. See the IANA web site for more information.</p> <p>Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select <b>Drop</b> to discard the frame(s). Select <b>Flooding</b> to send the frame(s) to all ports.</p>
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Immed. Leave	<p>Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port.</p> <p>Select this option if there is only one host connected to this port.</p>
Max Group Num.	<p>Select <b>Enable</b> and enter a number (0–255) to limit the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.</p>
IGMP Msg Limit	<p>Select <b>Enable</b> and enter a number (0–255) to limit the number of multicast frames this port is allowed to flow through. New multicast frames are dropped once more than the specified number of multicast frames flow into a port at one time.</p>
IGMP Filtering Profile	<p>Select the name of the IGMP filtering profile to use for this port. Otherwise, select <b>Default</b> to prohibit the port from joining any multicast group.</p> <p>You can create IGMP filtering profiles in the <b>Multicast &gt; Multicast Setting &gt; IGMP Filtering Profile</b> screen.</p>
IGMP Querier Mode	<p>The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port.</p> <p>Select <b>Auto</b> to have the Switch use the port as an IGMP query port if the port receives IGMP query packets.</p> <p>Select <b>Fixed</b> to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port.</p> <p>Select <b>Edge</b> to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.</p>

**Table 96** Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 24.4 IGMP Snooping VLAN

Click **Advanced Application > Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See [Section 24.1.4 on page 218](#) for more information on IGMP Snooping VLAN.

**Figure 132** Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

The following table describes the labels in this screen.

**Table 97** Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	<p>Select <b>auto</b> to have the Switch learn multicast group membership information of any VLANs automatically.</p> <p>Select <b>fixed</b> to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below.</p> <p>In either <b>auto</b> or <b>fixed</b> mode, the Switch can learn up to 16 VLANs (including up to three VLANs you configured in the <b>MVR</b> screen). For example, if you have configured one multicast VLAN in the <b>MVR</b> screen, you can only specify up to 15 VLANs in this screen.</p> <p>The Switch drops any IGMP control messages which do not belong to these 16 VLANs.</p> <p><b>Note:</b> You must also enable IGMP snooping in the <b>Multicast Setting</b> screen first.</p>
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.

**Table 97** Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN (continued)

LABEL	DESCRIPTION
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094.  Note: You cannot configure the same VLAN ID as in the <b>MVR</b> screen.
Add	Click <b>Add</b> to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click this to clear the fields.
Index	This is the number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column, then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 24.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile** link to display the screen as shown.

**Figure 133** Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

The following table describes the labels in this screen.

**Table 98** Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IPv4 or IPv6 address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IPv4 or IPv6 address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the <b>Start Address</b> and <b>End Address</b> fields.
Add	Click <b>Add</b> to save the profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the <b>Delete Profile</b> column, then click the <b>Delete</b> button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the <b>Delete Rule</b> column, then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete Profile/Delete Rule</b> check boxes.

## 24.6 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (1, 2 and 3) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

**Figure 134** MVR Network Example



### 24.6.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

### 24.6.2 MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

### 24.6.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

**Figure 135** MVR Multicast Television Example



## 24.7 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Application > Multicast > Multicast Setting > MVR** link to display the screen as shown next.

Note: You can create up to three multicast VLANs and up to 256 multicast rules on the Switch.

Note: Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

**Figure 136** Advanced Application > Multicast > Multicast Setting > MVR

The following table describes the related labels in this screen.

**Table 99** Advanced Application > Multicast > Multicast Setting > MVR

LABEL	DESCRIPTION
Behavior	Select <b>Snooping</b> to use the IGMP/MLD snooping mechanism for multicast VLAN traffic in this MVR network. IGMP/MLD snooping enables the Switch to handle multicast traffic more efficiently and effectively.  Select <b>Proxy</b> to use the IGMP/MLD proxy mechanism for multicast VLAN traffic in this MVR network. Select this to have the Switch reduce multicast traffic by sending IGMP/MLD host messages to a multicast router or server on behalf of all multicast hosts connected to the Switch.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).

**Table 99** Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
Mode	Specify the MVR mode on the Switch. Choices are <b>Dynamic</b> and <b>Compatible</b> . Select <b>Dynamic</b> to send IGMP reports to all MVR source ports in the multicast VLAN. Select <b>Compatible</b> to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the <b>Delete</b> column, then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 24.8 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.



Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

**Figure 137** Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

The following table describes the labels in this screen.

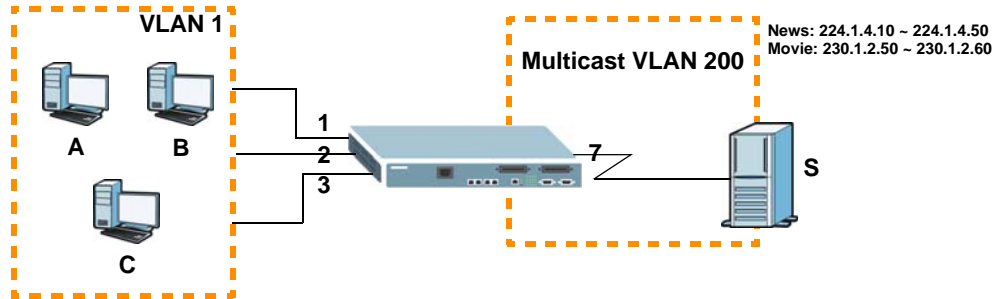
**Table 100** Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the <b>MVR</b> screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IPv4 or IPv6 multicast address of the multicast group in dotted decimal notation.  Refer to <a href="#">Section 24.1.1 on page 217</a> for more information on IP multicast addresses.
End Address	Enter the ending IPv4 or IPv6 multicast address of the multicast group in dotted decimal notation.  Enter the same IP address as the <b>Start Address</b> field if you want to configure only one IP address for a multicast group.  Refer to <a href="#">Section 24.1.1 on page 217</a> for more information on IP multicast addresses.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select <b>Delete Group</b> and click <b>Delete</b> to remove the selected entry(ies) from the table.  Select <b>Delete All</b> next to a multicast VLAN ID and click <b>Delete</b> to remove all multicast groups for that multicast VLAN from the table.
Cancel	Select <b>Cancel</b> to clear the checkbox(es) in the table.

## 24.8.1 MVR Configuration Example

The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN are able to receive the traffic.

Figure 138 MVR Configuration Example



To configure the MVR settings on the Switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 139 MVR Configuration Example

The screenshot shows the 'MVR' configuration page, specifically the 'Group Configuration' tab. The 'Active' checkbox is checked. The 'Name' field is 'Premium', 'Multicast VLAN ID' is '200', and '802.1p Priority' is '0'. The 'Mode' is set to 'Dynamic'. Below this is a table with columns: Port, Source Port, Receiver Port, None, and Tagging. Red circles highlight the configuration for port 7.

Port	Source Port	Receiver Port	None	Tagging
*		None		<input type="checkbox"/>
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

**Figure 140** MVR Group Configuration Example

**Group Configuration** MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
Movie	230.1.2.50	230.1.2.60

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	News	224.1.4.10	224.1.4.50	<input type="checkbox"/>	<input type="checkbox"/>

Delete Cancel

**Figure 141** MVR Group Configuration Example

**Group Configuration** MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
	0.0.0.0	0.0.0.0

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	Movie	230.1.2.50	230.1.2.60	<input type="checkbox"/>	<input type="checkbox"/>
	News	224.1.4.10	224.1.4.50		<input type="checkbox"/>

Delete Cancel

# Authentication and Accounting

This chapter describes how to configure authentication and accounting settings on the Switch.

## 25.1 Authentication, Authorization and Accounting

Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see [Section 25.1.2 on page 237](#)) and TACACS+ (Terminal Access Controller Access-Control System Plus, see [Section 25.1.2 on page 237](#)) as external authentication, authorization and accounting servers.

**Figure 142** AAA Server



### 25.1.1 Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way (See [Chapter 36 on page 327](#)).

## 25.1.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

**Table 101** RADIUS vs. TACACS+

	<b>RADIUS</b>	<b>TACACS+</b>
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

## 25.2 Authentication and Accounting Screens

To enable authentication on the Switch. First, configure your authentication server settings (RADIUS, TACACS+ or both) and then set up the authentication priority and accounting settings.

Click **Advanced Application > Auth and Acct** in the navigation panel to display the screen as shown.

**Figure 143** Advanced Application > Auth and Acct



### 25.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See [Section 25.1.2 on page 237](#) for more information on RADIUS servers and [Section 25.3 on page 245](#) for RADIUS attributes utilized by the

authentication and accounting feature on the Switch. Click on the **RADIUS Server Setup** link in the **Auth and Acct** screen to view the screen as shown.

**Figure 144** Advanced Application > Auth and Acct > RADIUS Server Setup

The following table describes the labels in this screen.

**Table 102** Advanced Application > Auth and Acct > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field is only valid if you configure multiple RADIUS servers.  Select <b>index-priority</b> and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server.  Select <b>round-robin</b> to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server.  If you are using <b>index-priority</b> for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IPv4 or IPv6 address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so.

**Table 102** Advanced Application > Auth and Acct > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click <b>Apply</b> .
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IPv4 or IPv6 address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for accounting is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click <b>Apply</b> .
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 25.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See [Section 25.1.2 on page 237](#) for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **Auth and Acct** screen to view the screen as shown.

**Figure 145** Advanced Application > Auth and Acct > TACACS+ Server Setup

The screenshot shows the 'TACACS+ Server Setup' configuration page. It is titled 'Auth and Acct' in the top right. The page is split into two main sections: 'Authentication Server' and 'Accounting Server'.  
 In the 'Authentication Server' section:  
 - 'Mode' is set to 'index-priority'.  
 - 'Timeout' is set to '30' seconds.  
 - A table lists two server entries:  
 | Index | IP Address | TCP Port | Shared Secret | Delete |  
 | 1 | 0.0.0.0 | 49 | |  |  
 | 2 | 0.0.0.0 | 49 | |  |  
 - 'Apply' and 'Cancel' buttons are at the bottom.  
 The 'Accounting Server' section has an identical layout with a 'Timeout' of 30 seconds and two server entries with IP 0.0.0.0 and port 49.

The following table describes the labels in this screen.

**Table 103** Advanced Application > Auth and Acct > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	This field is only valid if you configure multiple TACACS+ servers.  Select <b>index-priority</b> and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server.  Select <b>round-robin</b> to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server.  If you are using <b>index-priority</b> for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IPv4 or IPv6 address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is <b>49</b> . You need not change this value unless your network administrator instructs you to do so.



**Table 103** Advanced Application > Auth and Acct > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click <b>Apply</b> .
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IPv4 or IPv6 address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for accounting is <b>49</b> . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click <b>Apply</b> .
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 25.2.3 Authentication and Accounting Setup

Use this screen to configure authentication and accounting settings on the Switch. Click on the **Auth and Acct Setup** link in the **Auth and Acct** screen to view the screen as shown.

**Figure 146** Advanced Application > Auth and Acct > Auth and Acct Setup

The screenshot shows the 'Auth and Acct Setup' configuration page. At the top, there's a title bar with 'Auth and Acct Setup' and a link to 'Auth and Acct'. Below this, the 'Authentication' section contains a table with the following data:

Type	Method 1	Method 2	Method 3
Privilege Enable	local	-	-
Login	local	-	-

The 'Accounting' section includes an 'Update Period' field set to 0 minutes. Below it is another table with the following data:

Type	Active	Broadcast	Mode	Method	Privilege
System	<input type="checkbox"/>	<input type="checkbox"/>	-	radius	-
Exec	<input type="checkbox"/>	<input type="checkbox"/>	start-stop	radius	-
Dot1x	<input type="checkbox"/>	<input type="checkbox"/>	start-stop	radius	-
Commands	<input type="checkbox"/>	<input type="checkbox"/>	stop-only	tacacs+	0

At the bottom of the screen are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 104** Advanced Application > Auth and Acct > Authentication Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Privilege Enable	<p>These fields specify which database the Switch should use (first, second and third) to authenticate access privilege level for administrator accounts (users for Switch management).</p> <p>Configure the access privilege of accounts via commands (See the CLI Reference Guide) for <b>local</b> authentication. The <b>TACACS+</b> and <b>RADIUS</b> are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>You can specify up to three methods for the Switch to authenticate the access privilege level of administrators. The Switch checks the methods in the order you configure them (first <b>Method 1</b>, then <b>Method 2</b> and finally <b>Method 3</b>). You must configure the settings in the <b>Method 1</b> field. If you want the Switch to check other sources for access privilege level specify them in <b>Method 2</b> and <b>Method 3</b> fields.</p> <p>Select <b>local</b> to have the Switch check the access privilege configured for local authentication.</p> <p>Select <b>radius</b> or <b>tacacs+</b> to have the Switch check the access privilege via the external servers.</p>

**Table 104** Advanced Application > Auth and Acct > Authentication Setup (continued)

LABEL	DESCRIPTION
Login	<p>These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management).</p> <p>Configure the local user accounts in the <b>Access Control &gt; Logins</b> screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first <b>Method 1</b>, then <b>Method 2</b> and finally <b>Method 3</b>). You must configure the settings in the <b>Method 1</b> field. If you want the Switch to check other sources for administrator accounts, specify them in <b>Method 2</b> and <b>Method 3</b> fields.</p> <p>Select <b>local</b> to have the Switch check the administrator accounts configured in the <b>Access Control &gt; Logins</b> screen.</p> <p>Select <b>radius</b> to have the Switch check the administrator accounts configured via your RADIUS server.</p> <p>Select <b>tacacs+</b> to have the Switch check the administrator accounts configured via your TACACS+ server.</p>
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the <b>start-stop</b> option for the <b>Exec</b> or <b>Dot1x</b> entries.
Type	<p>The Switch supports the following types of events to be sent to the accounting server(s):</p> <p><b>System:</b> Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled</p> <p><b>Exec:</b> Configure the Switch to send information when an administrator logs in and logs out via the console port, Telnet or SSH.</p> <p><b>Dot1x:</b> Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session.</p> <p><b>Commands:</b> Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.</p>
Active	Select this to activate accounting for a specified event types.
Broadcast	<p>Select this to have the Switch send accounting information to all configured accounting servers at the same time.</p> <p>If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.</p>
Mode	<p>The Switch supports two modes of recording login events. Select:</p> <p><b>start-stop:</b> to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the <b>Update Period</b>), and when a user ends a session.</p> <p><b>stop-only:</b> to have the Switch send information to the accounting server only when a user ends a session.</p>
Method	<p>Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events.</p> <p>TACACS+ is the only method for recording <b>Commands</b> type of event.</p>

**Table 104** Advanced Application > Auth and Acct > Authentication Setup (continued)

LABEL	DESCRIPTION
Privilege	This field is only configurable for <b>Commands</b> type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 25.2.4 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (See the CLI Reference Guide for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID:** An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type:** A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data:** A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch.

**Table 105** Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = <b>890</b> Vendor-Type = <b>1</b> Vendor-data = ingress rate (Kbps in decimal format)
Egress Bandwidth Assignment	Vendor-Id = <b>890</b> Vendor-Type = <b>2</b> Vendor-data = egress rate (Kbps in decimal format)

**Table 105** Supported VSAs

FUNCTION	ATTRIBUTE
Privilege Assignment	Vendor-ID = <b>890</b> Vendor-Type = <b>3</b> Vendor-Data = " <b>shell:priv-lvl=N</b> "  or  Vendor-ID = <b>9</b> (CISCO) Vendor-Type = <b>1</b> (CISCO-AVPAIR) Vendor-Data = " <b>shell:priv-lvl=N</b> "  where N is a privilege level (from 0 to 14).  Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

### 25.2.4.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

**Table 106** Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = <b>VLAN(13)</b> Tunnel-Medium-Type = <b>802(6)</b> Tunnel-Private-Group-ID = VLAN ID  Note: You must also create a VLAN with the specified VID on the Switch.

## 25.3 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication and accounting elements in a user profile, which is stored on the RADIUS server. This section lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for more information about RADIUS attributes used for accounting.

This section lists the attributes used by authentication functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

### 25.3.1 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

### 25.3.1.1 Attributes Used for Authenticating Privilege Access

User-Name

- The format of the User-Name attribute is **\$enab#\$**, where # is the privilege level (1-14).

User-Password

NAS-Identifier

NAS-IP-Address

### 25.3.1.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

### 25.3.1.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

## 25.3.2 Attributes Used for Accounting

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

### 25.3.2.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID

- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 2007041917210300000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

### 25.3.2.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

**Table 107** RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

**Table 108** RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Calling-Station-Id	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

### 25.3.2.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

**Table 109** RADIUS Attributes-Exec Events via 802.1x

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-IP-Address	Y	Y	Y
NAS-Port	Y	Y	Y
Class	Y	Y	Y
Called-Station-Id	Y	Y	Y

**Table 109** RADIUS Attributes-Exec Events via 802.1x

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Calling-Station-Id	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-Port-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Input-Octets		Y	Y
Acct-Output-Octets		Y	Y
Acct-Session-Time		Y	Y
Acct-Input-Packets		Y	Y
Acct-Output-Packets		Y	Y
Acct-Terminate-Cause			Y
Acct-Input-Gigawords		Y	Y
Acct-Output-Gigawords		Y	Y



# IP Source Guard

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

## 26.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

### 26.1.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

#### 26.1.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

### 26.1.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

**Figure 147** DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-...-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

### 26.1.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See [Chapter 35 on page 311](#) for more information about DHCP relay option 82.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings ([Chapter 35 on page 311](#)).

### 26.1.1.4 Configuring DHCP Snooping

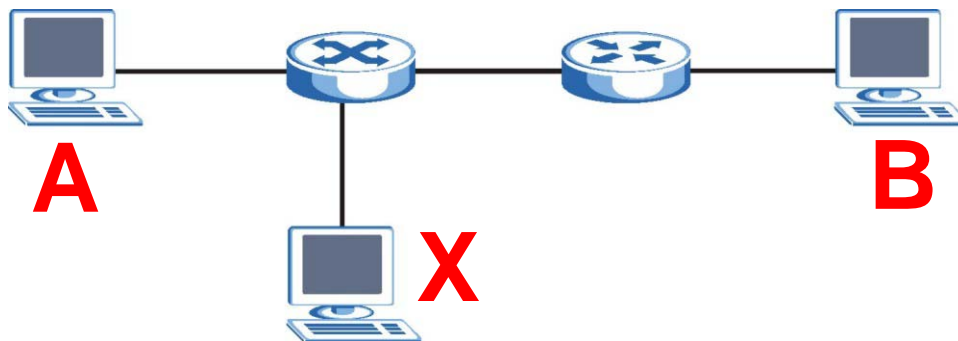
Follow these steps to configure DHCP snooping on the Switch.

- 1 Enable DHCP snooping on the Switch.
- 2 Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.
- 3 Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
- 4 Configure static bindings.

## 26.1.2 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

**Figure 148** Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

### 26.1.2.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters ([Chapter 13 on page 158](#)).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

### 26.1.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

### 26.1.2.3 Syslog

The Switch can send syslog messages to the specified syslog server ([Chapter 39 on page 358](#)) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

### 26.1.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

- 1 Configure DHCP snooping. See [Section 26.1.1.4 on page 251](#).

Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

- 2 Enable ARP inspection on each VLAN.
- 3 Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

## 26.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

**Figure 149** IP Source Guard



The following table describes the labels in this screen.

**Table 110** IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, <b>2d3h4m5s</b> means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays <b>infinity</b> if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. <b>static</b> : This binding was learned from information provided manually by an administrator. <b>dhcp-snooping</b> : This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

## 26.3 IP Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN

ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

**Figure 150** IP Source Guard Static Binding

The following table describes the labels in this screen.

**Table 111** IP Source Guard Static Binding

LABEL	DESCRIPTION
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select <b>Any</b> .
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. <b>static</b> : This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select this, and click <b>Delete</b> to remove the specified entry.
Cancel	Click this to clear the <b>Delete</b> check boxes above.

## 26.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

**Figure 151** DHCP Snooping

DHCP Snooping		<a href="#">Configure</a>	<a href="#">IPSG</a>
<b>Database Status</b>			
Description	Status		
Agent URL			
Write delay timer	300	seconds	
Abort timer	300	seconds	
<b>Agent running</b>			
Agent running	None		
Delay timer expiry	Not Running		
Abort timer expiry	Not Running		
<b>Last succeeded time</b>			
Last succeeded time	None		
<b>Last failed time</b>			
Last failed time	None		
<b>Last failed reason</b>			
Last failed reason	No failure recorded		
<b>Times</b>			
Total attempts	0		
Startup failures	0		
Successful transfers	0		
Failed transfers	0		
Successful reads	0		
Failed reads	0		
Successful writes	0		
Failed writes	0		
<b>Database detail</b>			
Description	Status		
First successful access	None		
<b>Last ignored bindings counters</b>			
Binding collisions	0		
Invalid interfaces	0		
Parse failures	0		
Expired leases	0		
Unsupported vlans	0		
Last ignored time	None		
<b>Total ignored bindings counters</b>			
Binding collisions	0		
Invalid interfaces	0		
Parse failures	0		
Expired leases	0		
Unsupported vlans	0		

The following table describes the labels in this screen.

**Table 112** DHCP Snooping

LABEL	DESCRIPTION
Database Status	This section displays the current settings for the DHCP snooping database. You can configure them in the <b>DHCP Snooping Configure</b> screen. See <a href="#">Section 26.5 on page 257</a> .
Agent URL	This field displays the location of the DHCP snooping database.
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.
Agent running	This field displays the status of the current update or access of the DHCP snooping database.  <b>none</b> : The Switch is not accessing the DHCP snooping database. <b>read</b> : The Switch is loading dynamic bindings from the DHCP snooping database. <b>write</b> : The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays <b>Not Running</b> if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays <b>Not Running</b> if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.
Successful writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.



**Table 112** DHCP Snooping (continued)

LABEL	DESCRIPTION
Failed writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.
Last ignored bindings counters	This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total ignored bindings counters	This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

## 26.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are

still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

**Figure 152** DHCP Snooping Configure

The following table describes the labels in this screen.

**Table 113** DHCP Snooping Configure

LABEL	DESCRIPTION
Active	Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports.  Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
DHCP Vlan	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN.  Note: You have to enable DHCP snooping on the DHCP VLAN too.  You can enable <b>Option82</b> in the <b>DHCP Snooping VLAN Configure</b> screen ( <a href="#">Section 26.5.2 on page 260</a> ) to help the DHCP servers distinguish between DHCP requests from different VLAN.  Select <b>Disable</b> if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database	If <b>Timeout interval</b> is greater than <b>Write delay interval</b> , it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: <b>tftp://{domain name or IP address}/directory, if applicable/file name</b> ; for example, <b>tftp://192.168.10.1/database.txt</b> .
Timeout interval	Enter how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.

**Table 113** DHCP Snooping Configure (continued)

LABEL	DESCRIPTION
Write delay interval	Enter how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click <b>Renew</b> if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in <b>Agent URL</b> .  When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the <b>Binding collisions</b> counter in the <b>DHCP Snooping</b> screen (Section 26.4 on page 255).
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

## 26.5.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: If DHCP snooping is enabled but there are no trusted ports, DHCP requests cannot reach the DHCP server.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

**Figure 153** DHCP Snooping Port Configure

Port	Server Trusted state	Rate (pps)
*	Untrusted	
1	Untrusted	0
2	Untrusted	0
3	Untrusted	0
4	Untrusted	0
5	Untrusted	0
6	Untrusted	0
7	Untrusted	0
8	Untrusted	0
9	Untrusted	0
10	Untrusted	0
11	Untrusted	0
12	Untrusted	0
13	Untrusted	0
14	Untrusted	0
15	Untrusted	0
16	Untrusted	0
17	Untrusted	0
18	Untrusted	0
19	Untrusted	0
20	Untrusted	0
21	Untrusted	0
22	Untrusted	0
23	Untrusted	0
24	Untrusted	0
25	Untrusted	0
26	Untrusted	0

The following table describes the labels in this screen.

**Table 114** DHCP Snooping Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Server Trusted state	Select whether this port is a trusted port ( <b>Trusted</b> ) or an untrusted port ( <b>Untrusted</b> ).  Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.  Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations:  The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).  The source MAC address and source IP address in the packet do not match any of the current bindings.  The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.  The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

## 26.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information ([Chapter 35 on page 311](#)) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

**Figure 154** DHCP Snooping VLAN Configure

The screenshot shows the 'DHCP Snooping VLAN Configure' interface. At the top, there is a title bar with a 'Configure' link. Below the title bar, there is a 'Show VLAN' section with 'Start VID' and 'End VID' input fields, and an 'Apply' button. The main part of the screen is a table with the following columns: VID, Enabled, Option82, SPV, Delimiter, Information, and Remote ID. The first row of the table has the following values: VID: \*, Enabled: No (dropdown), Option82: , SPV: private (dropdown), Delimiter: none (dropdown), Information: , and Remote ID: . At the bottom of the screen, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 115** DHCP Snooping VLAN Configure

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select <b>Yes</b> to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports.  If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
Option82	Select this to have the Switch add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the <b>DHCP Snooping Configure</b> screen. See <a href="#">Section 26.5 on page 257</a> .
SPV	Select the variables that you want the Switch to generate and add in the DHCP requests. The variable options include <b>SP</b> , <b>SV</b> , <b>PV</b> and <b>SPV</b> which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively in ASCII code. Alternatively, select <b>private</b> to have the Switch use the DHCP relay option 82 old format (slot-port-VLAN) in binary. The Switch uses a zero for the slot value in the DHCP requests. An example of the port number is 1 if you select <b>private</b> while it is 31 in ASCII code if you select <b>SP</b> , <b>SV</b> or <b>SPV</b> .
Delimiter	Select a delimiter to separate the option 82 information, slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Information	Select this to have the Switch add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can configure the system name in the <b>General Setup Configure</b> screen. See <a href="#">Chapter 8 on page 70</a> . You can specify the DHCP VLAN in the <b>DHCP Snooping Configure</b> screen. See <a href="#">Section 26.5 on page 257</a> .
Remote ID	Select this to have the Switch also add the receiving port name as the remote ID to DHCP requests. Clear this to not add remote IDs to DHCP requests.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

## 26.6 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address

and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

**Figure 155** ARP Inspection Status

ARP Inspection Status [VLAN Status](#) [Log Status](#) [Configure](#) [IPSG](#)

Total number of filters = 0

Index	MAC Address	VID	Port	Expiry (sec)	Reason	Delete
*	-	-	-	-	-	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 116** ARP Inspection Status

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually ( <b>Delete</b> ).
Reason	This field displays the reason the ARP packet was discarded. <b>MAC+VLAN:</b> The MAC address and VLAN ID were not in the binding table. <b>IP:</b> The MAC address and VLAN ID were in the binding table, but the IP address was not valid. <b>Port:</b> The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this, and click <b>Delete</b> to remove the specified entry.
Cancel	Click this to clear the <b>Delete</b> check boxes above.
Change Pages	Click <b>Previous Page</b> or <b>Next Page</b> to show the previous/next screen if all status information cannot be seen in one screen.

## 26.6.1 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

**Figure 156** ARP Inspection VLAN Status

The following table describes the labels in this screen.

**Table 117** ARP Inspection VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID ( <b>Start VID</b> ) and the highest VLAN ID ( <b>End VID</b> ) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

## 26.6.2 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

**Figure 157** ARP Inspection Log Status



The following table describes the labels in this screen.

**Table 118** ARP Inspection Log Status

LABEL	DESCRIPTION
Clearing log status table	Click <b>Apply</b> to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called <b>overflow</b> with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the <b>ARP Inspection Configure</b> screen. See <a href="#">Section 26.7 on page 265</a> .
Reason	<p>This field displays the reason the log message was generated.</p> <p><b>dhcp deny:</b> An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID.</p> <p><b>static deny:</b> An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID.</p> <p><b>deny:</b> An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID.</p> <p><b>dhcp permit:</b> An ARP packet was forwarded because it matched a dynamic binding.</p> <p><b>static permit:</b> An ARP packet was forwarded because it matched a static binding.</p> <p>In the <b>ARP Inspection VLAN Configure</b> screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See <a href="#">Section 26.7.2 on page 268</a>.</p>
Time	This field displays when the log message was generated.



## 26.7 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

**Figure 158** ARP Inspection Configure

The following table describes the labels in this screen.

**Table 119** ARP Inspection Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1~2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Enter 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1~1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified <b>Syslog rate</b> and <b>Log interval</b> .  If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click <b>Clearing log status table</b> in the <b>ARP Inspection Log Status</b> screen to clear the log and reset this counter. See <a href="#">Section 26.6.2 on page 264</a> .

**Table 119** ARP Inspection Configure (continued)

LABEL	DESCRIPTION
Syslog rate	<p>Enter the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the <b>Log Interval</b>. You must configure the syslog server (<a href="#">Chapter 39 on page 358</a>) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server.</p> <p>The relationship between <b>Syslog rate</b> and <b>Log interval</b> is illustrated in the following examples:</p> <p>4 invalid ARP packets per second, <b>Syslog rate</b> is 5, <b>Log interval</b> is 1: the Switch sends 4 syslog messages every second.</p> <p>6 invalid ARP packets per second, <b>Syslog rate</b> is 5, <b>Log interval</b> is 2: the Switch sends 5 syslog messages every 2 seconds.</p>
Log interval	<p>Enter how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See <b>Syslog rate</b> for an example of the relationship between <b>Syslog rate</b> and <b>Log interval</b>.</p>
Apply	<p>Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click this to reset the values in this screen to their last-saved values.</p>

## 26.7.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To

open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

**Figure 159** ARP Inspection Port Configure

Port	Trusted State	Limit	
		Rate (pps)	Burst interval (seconds)
*	Untrusted		
1	Untrusted	15	1
2	Untrusted	15	1
3	Untrusted	15	1
4	Untrusted	15	1
5	Untrusted	15	1
6	Untrusted	15	1
7	Untrusted	15	1
8	Untrusted	15	1
9	Untrusted	15	1
10	Untrusted	15	1
25	Untrusted	15	1
26	Untrusted	15	1

Apply Cancel

The following table describes the labels in this screen.

**Table 120** ARP Inspection Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port ( <b>Trusted</b> ) or an untrusted port ( <b>Untrusted</b> ). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: The sender's information in the ARP packet does not match any of the current bindings. The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	These settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.

**Table 120** ARP Inspection Port Configure (continued)

LABEL	DESCRIPTION
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval.  Enter the length (1-15 seconds) of the burst interval.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

## 26.7.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

**Figure 160** ARP Inspection VLAN Configure

The following table describes the labels in this screen.

**Table 121** ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select <b>Yes</b> to enable ARP inspection on the VLAN. Select <b>No</b> to disable ARP inspection on the VLAN.

**Table 121** ARP Inspection VLAN Configure (continued)

LABEL	DESCRIPTION
Log	<p>Specify when the Switch generates log messages for receiving ARP packets from the VLAN.</p> <p><b>None:</b> The Switch does not generate any log messages when it receives an ARP packet from the VLAN.</p> <p><b>Deny:</b> The Switch generates log messages when it discards an ARP packet from the VLAN.</p> <p><b>Permit:</b> The Switch generates log messages when it forwards an ARP packet from the VLAN.</p> <p><b>All:</b> The Switch generates log messages every time it receives an ARP packet from the VLAN.</p>
Apply	<p>Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click this to reset the values in this screen to their last-saved values.</p>

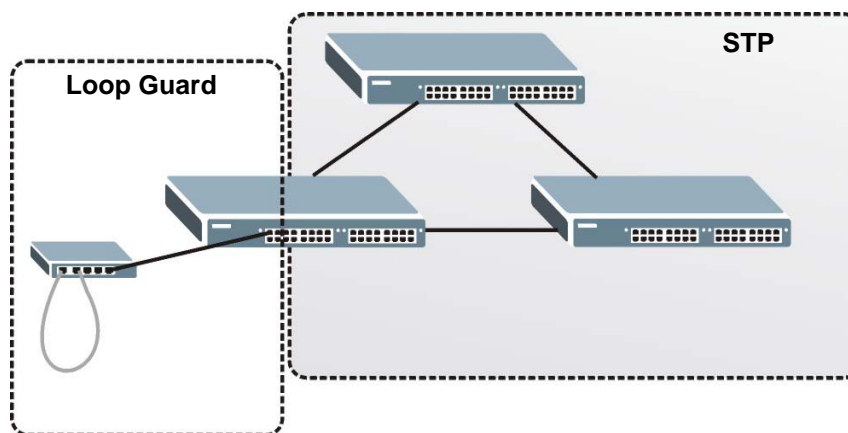
## Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

### 27.1 Loop Guard Overview

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

**Figure 161** Loop Guard vs. STP



Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

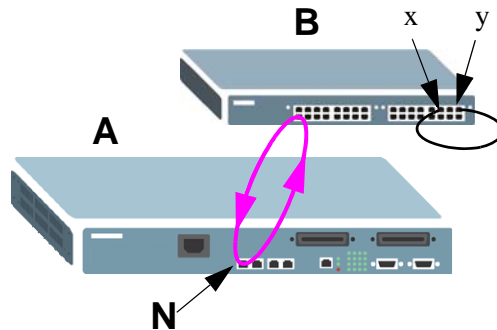
If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on the Switch **A** connected to another switch **B**. Switch **B** has mistakenly two ports, **x** and **y**, connected to each other. It forms a loop. When switch **B** receives

broadcast or multicast frames, they will be broadcasted again to senders including the port **N** on the Switch **A**.

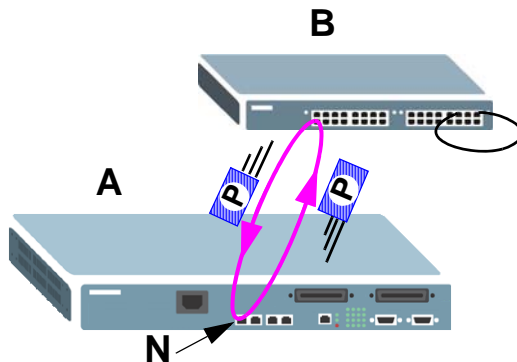
**Figure 162** Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

Loop guard can be enabled on both Ethernet ports or xDSL ports. In the following figure, Ethernet port **N** has loop guard enabled on the Switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

**Figure 163** Loop Guard - Probe Packet

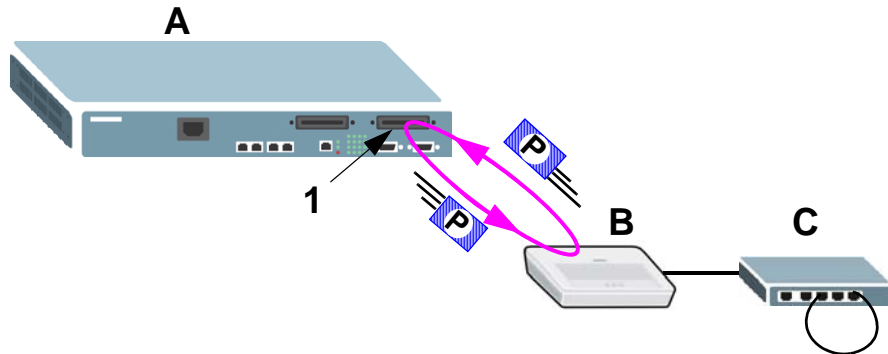


The Switch also shuts down port **N** if the probe packet returns to Switch **A** on any other port. In other words loop guard also protects against standard network loops.

The following figure illustrates the Switch **A**, a subscriber device **B** and another switch **C** forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from an xDSL port **1** and returns also on port **1**. As long as loop guard is enabled on

port 1, the Switch will shut down port 1 if it detects that the probe packet has returned to the Switch.

**Figure 164** Loop Guard - Network Loop



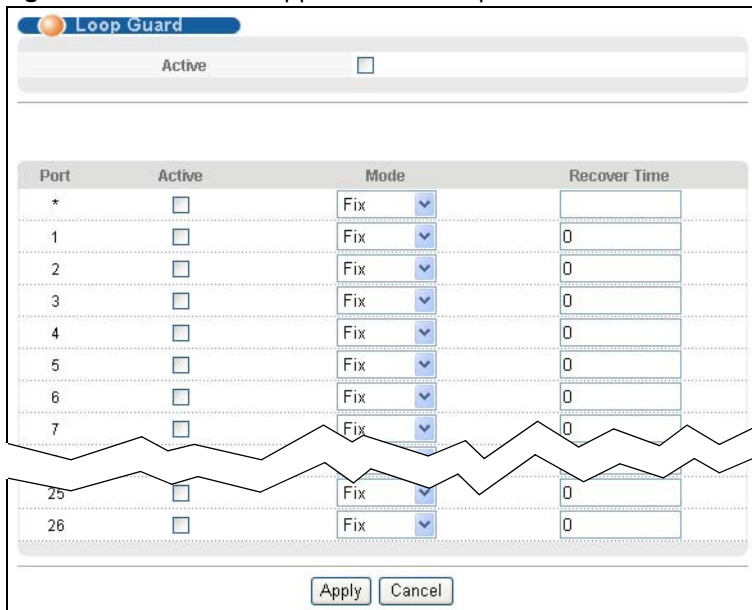
Note: After resolving the loop problem on your network you can re-activate the disabled port via the Web Configurator (see [Section 8.9 on page 82](#)) or via commands (See the CLI Reference Guide).

## 27.2 Loop Guard Setup

Click **Advanced Application > Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

**Figure 165** Advanced Application > Loop Guard





The following table describes the labels in this screen.

**Table 122** Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	<p>Select this option to enable loop guard on the Switch.</p> <p>The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.</p>
Port	This field displays the port number.
*	<p>Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis.</p> <p><b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.</p>
Active	<p>Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected to is in loop state the Switch will shut down this port.</p> <p>Clear this check box to disable the loop guard feature.</p>
Mode	<p>Select the port mode for loop guard.</p> <p>If you select <b>Fix</b>, the Switch shuts down the port when the Switch detects that packets sent out on the port loop back to the Switch. To activate the port again, you need to manually enable the port in the <b>Port Setup</b> screen.</p> <p>If you select <b>Dynamic</b>, the Switch shuts down the port if the Switch detects that packets sent out on the port loop back to the Switch. The port becomes active automatically after the time you specified in the <b>Recover Time</b> field.</p>
Recover Time	Enter the time (in seconds) the port in dynamic mode waits to become active again after shut down by the Switch.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

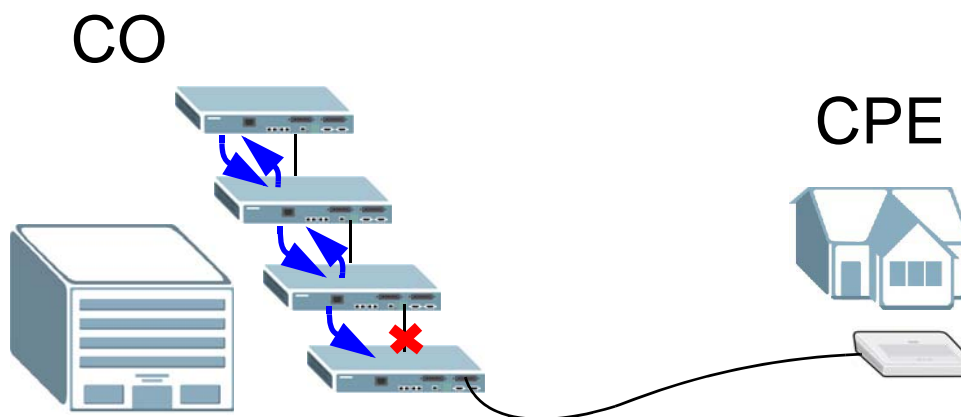
This chapter explains the **Connectivity Fault Management (CFM)** screens.

## 28.1 CFM Overview

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscribers' network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

The figure shown below is an example of a connection fault between switches on the LAN. CFM can be used to identify and management this kind of connection problem.

**Figure 166** Management for any Fault in Bridges



### 28.1.1 How CFM Works

To enable CFM, pro-active Connectivity Check Messages (CCMs) between two CFM-aware devices in the same MD (Maintenance Domain) network. An MA (Maintenance Association) defines a VLAN and associated ports on the device under an MD level. In this MA, a port can be an MEP (Maintenance End Point) port or an MIP (Maintenance Intermediate Point) port.

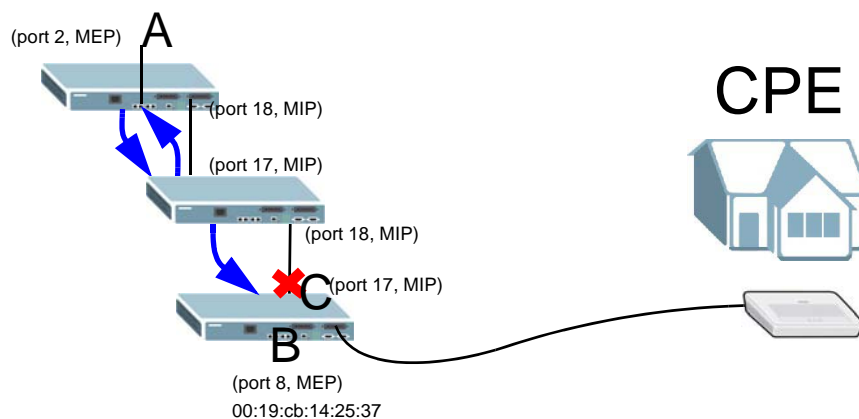
- MEP port - has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor switches' CCMs within an MA.
- MIP port - forwards the CCMs, Loop Back Messages (LBMs) and Link Trace Messages (LTMs).

CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its LBR (Loop Back Response) from its target after it sends the LBM (Loop Back Message). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. In the link trace test, MIP ports also send the LTR (Link Trace Response) to response the source MEP port's LTM (Link Trace Message). If an MIP or MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report. Refer to the [Section 44.1 on page 370](#) to perform CFM actions.

An example is shown next. A user reports his VDSL line link down. To check the problem, the administrator starts the link trace test from the **A** which is an MEP port to the **B** which is also an MEP port. Each aggregation MIP port between switches response the LTM packets and also forwards them to the next port. A fault occurs in the port **C**. **A** discovers the fault since it just gets the LTR packets from the ports flowing before the port **C**.

**Figure 167** MIP and MEP example



## 28.2 CFM MA

Click **Advanced Application** and **CFM** to open this screen. Use this screen to create an MA (Maintenance Association) under an MD level. You have to specify a name, a VLAN ID and its member ports. Refer to [Section 28.1 on page 274](#) for more information about CFM.

**Note:** You have to create a CFM MD first before you create an MA.

**Figure 168** CFM MA

The following table describes the labels in this screen.

**Table 123** CFM MA

LABEL	DESCRIPTION
MD level	Select a level (0-7) you want to create an MA under.  Note: You have to create an MD first by clicking the <b>CFM MD</b> link.
MA Name	Type a descriptive name (up to 40 printable ASCII characters) for this MA. This is for identification purpose.
MA Vlan ID	Type a VLAN ID (0-4096) for this MA.  Note: Make sure the VLAN ID has existed before you use it for the MA VLAN ID.
CFM Enable	Select this to activate the CFM.
Port	This field displays the port number.
Active	Select this to activate a port in this MA.
Name	This field displays the MA name.
MP Type	Select a port type such as <b>MEP</b> (Maintenance End Point) or <b>MIP</b> (Maintenance Intermediate Point). Or leave it as default ( <b>None</b> ).
MEP ID	Enter an ID number (1-8191) for this MEP port. Each MEP port needs a unique ID number within an MD. The MEP ID is to identify an MEP port used when you create a CFM action. See <a href="#">Section 44.1 on page 370</a> .
Add	Click <b>Add</b> to add the settings as a new entry in the summary table below.
Cancel	Click <b>Cancel</b> to reset the fields.
Clear	Click <b>Clear</b> to start configuring the screen again.
Index	This field displays the index number for the record in this summary table.

**Table 123** CFM MA

LABEL	DESCRIPTION
MA Name	This field displays the descriptive name of the MA.
MA VID	This field displays the ID number of the MA VLAN group.
MEP Port	This field lists individual MEP ports in this MA VLAN group.
MIP Port	This field lists individual MIP ports in this MA VLAN group.
Delete	Select rules to remove in the <b>Delete</b> column and then click the <b>Delete</b> button to remove them.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 28.3 CFM MD

Click the link **CFM MD** on the **CFM MA** screen to open this screen. Use this screen to create an MD and specify an MD level. Refer to [Section 28.1 on page 274](#) for more information about CFM.

**Figure 169** CFM MD

The following table describes the labels in this screen.

**Table 124** CFM MD

LABEL	DESCRIPTION
MD Name	Type a name (up to 40 printable ASCII characters) for this MD. This is for identification purposes.
MD Level	Type a level number (0-7) for this MD.
Add	Click <b>Add</b> to add the settings as a new entry in the summary table below.
Cancel	Click <b>Cancel</b> to reset the fields.
Clear	Click <b>Clear</b> to start configuring the screen again.
Index	This field displays the index number for the record in this summary table.
MD Name	This field displays the descriptive name of the MD.
MD Level	This field displays the level number of the MD.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

# VLAN Mapping

This chapter shows you how to configure VLAN mapping on the Switch.

## 29.1 VLAN Mapping Overview

With VLAN mapping enabled, the Switch can map the VLAN ID and priority level of packets received from a private network to those used in the service provider's network.

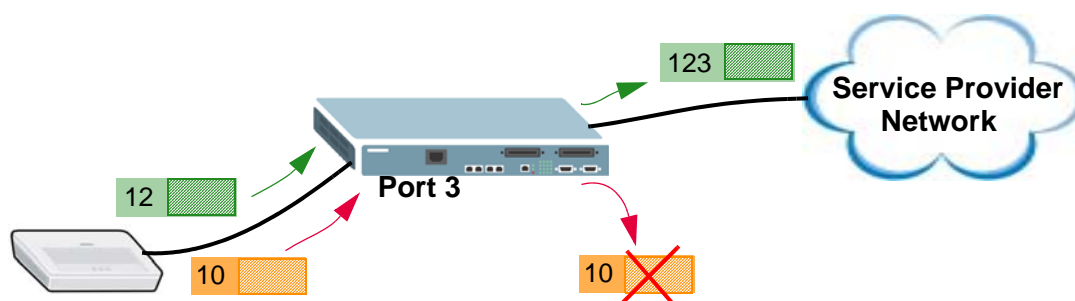
The Switch checks incoming traffic from the non-management ports against the VLAN mapping table first, the MAC learning table and then the VLAN table before forwarding them through the Gigabit uplink port. When VLAN mapping is enabled, the Switch discards the tagged packets that do not match an entry in the VLAN mapping table. If the incoming packets are untagged, the Switch adds a PVID based on the VLAN setting.

Note: You can not enable VLAN mapping and VLAN stacking at the same time.

### 29.1.1 VLAN Mapping Example

In the following example figure, packets that carry VLAN ID 12 and are received on port 3 match a pre-configured VLAN mapping rule. The Switch translates the VLAN ID from 12 into 123 before forwarding the packets. Any incoming packets carrying a VLAN tag other than 12 (such as 10) and received on port 3 will be dropped if you select to drop the packets that do not match the mapping rule (**Drop Miss**).

**Figure 170** VLAN mapping example



## 29.2 Enabling VLAN Mapping

Click **Advanced Application** and then **VLAN Mapping** in the navigation panel to display the screen as shown.

**Figure 171** VLAN Mapping

Port	Active	Drop Miss
*	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>
26	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 125** VLAN Mapping

LABEL	DESCRIPTION
Active	Select this option to enable VLAN mapping on the Switch.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis.  Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the VLAN mapping feature on this port. Clear this check box to disable the VLAN mapping feature.
Drop Miss	Select this check box to discard the incoming packets that do not match any VLAN mapping rules on this port. Otherwise, clear the check box to forward the packets without replacing the VLAN tag.  The Switch forwards any outgoing packets even when they do not match a VLAN mapping rule.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 29.3 Configuring VLAN Mapping

Click the **VLAN Mapping Configure** link in the **VLAN Mapping** screen to display the screen as shown. Use this screen to enable and edit the VLAN mapping rule(s).

**Figure 172** VLAN Mapping Configuration

The following table describes the labels in this screen.

**Table 126** VLAN Mapping Configuration

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	Type a port to be included in this rule.
VID	Enter a VLAN ID from 1 to 4094. This is the VLAN tag carried in the packets and will be translated into the VID you specified in the <b>Translated VID</b> field.
Translated VID	Enter a VLAN ID (from 1 to 4094) into which the customer VID carried in the packets will be translated.
Priority	Select a priority level (from 0 to 7). This is the priority level that replaces the customer priority level in the tagged packets or adds to the untagged packets. Select the <b>Replace Original</b> check box to have the Switch change the customer priority to what you select here. If you clear the <b>Replace Original</b> checkbox, the Switch keeps the original customer priority.
Add	Click <b>Add</b> to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Index	This is the number of the VLAN mapping entry in the table.
Active	This shows whether this entry is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied.
VID	This is the customer VLAN ID in the incoming packets.
Translated VID	This is the VLAN ID that replaces the customer VLAN ID in the tagged packets.
Priority	This is the priority level that replaces the customer priority level in the tagged packets.



**Table 126** VLAN Mapping Configuration (continued)

LABEL	DESCRIPTION
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.

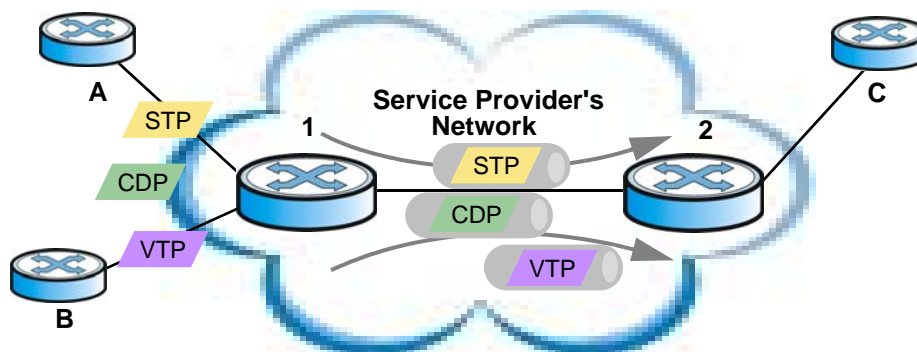
## Layer 2 Protocol Tunneling

This chapter shows you how to configure layer 2 protocol tunneling on the Switch.

### 30.1 Layer 2 Protocol Tunneling Overview

Layer 2 protocol tunneling (L2PT) is used on the service provider's edge devices. L2PT allows edge switches (**1** and **2** in the following figure) to tunnel layer 2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) and VTP (VLAN Trunking Protocol) packets between customer switches (**A**, **B** and **C** in the following figure) connected through the service provider's network. The edge switch encapsulates layer 2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

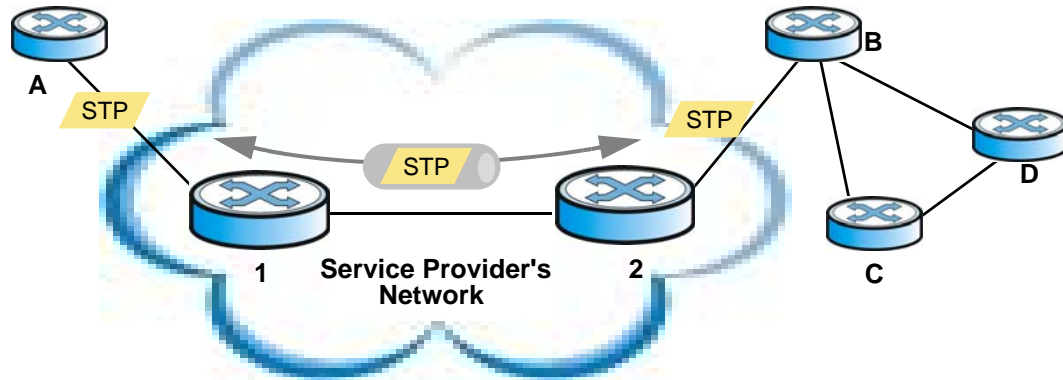
**Figure 173** Layer 2 Protocol Tunneling Network Scenario



In the following example, if you enable L2PT for STP, you can have switches **A**, **B**, **C** and **D** in the same spanning tree, even though switch **A** is not directly connected to switches **B**, **C** and **D**. Topology change information can be propagated throughout the service provider's network.

To emulate a point-to-point topology between two customer switches at different sites, such as **A** and **B**, you can enable protocol tunneling on edge switches **1** and **2** for PAGP (Port Aggregation Protocol), LACP or UDLD (UniDirectional Link Detection).

**Figure 174** L2PT Network Example



### 30.1.1 Layer 2 Protocol Tunneling Mode

Each port can have two layer 2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in [Figure 174 on page 283](#)) and connected to a customer switch (**A** or **B**). Incoming layer 2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- The **Tunnel** port is an egress port at the edge of the service provider's network and connected to another service provider's switch. Incoming encapsulated layer 2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

## 30.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application > Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

**Figure 175** Layer 2 Protocol Tunneling

Port	CDP	STP	VTP	Point to Point			Mode
				PAGP	LACP	UDLD	
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access
26	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access

The following table describes the labels in this screen.

**Table 127** Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer 2 protocol tunneling on the Switch.
Destination MAC Address	Specify an MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets.  Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network.  Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.

**Table 127** Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.
Point to Point	<p>The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology.</p> <p>Both PAgP and UDLD are Cisco's proprietary data link layer protocols. PAgP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.</p>
PAGP	Select this option to have the Switch send PAgP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically creates and manages trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	<p>Select <b>Access</b> to have the Switch encapsulate the incoming layer 2 protocol packets and forward them to the tunnel port(s). Select <b>Access</b> for ingress ports at the edge of the service provider's network.</p> <p>You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only.</p> <p>Select <b>Tunnel</b> for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer 2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the service(s) is not enabled on an access port, the protocol packets are dropped.</p>
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# DoS Prevention

This chapter explains the **DoS Prevention** screens.

## 31.1 DoS Prevention Overview

To protect against DoS (Denial of Service) attacks such as SYN flooding and Ping of Death, the Switch can use filtering actions to determine when to start dropping packets that may potentially be associated with a DoS attack.

## 31.2 Configuring DoS Prevention

Click **Advanced Application > DoS Prevention** in the navigation panel to display the screen as shown.

**Figure 176** DoS Prevention

**DoS Prevention**

Active

Action

Mac

If packets with source Mac address equals destination Mac address, drop them.

IP

If packets with source IP address equals destination IP address, drop them.

ICMP

If the packets are fragmented ICMP packets, drop them.

TCP

Check TCP SYN packet with source port values are always 0, drop them.

TCP fragments with offset value of 1 are dropped.

TCP packets with control flags equals 0 and sequence number equals 0, drop them.

TCP packets with source port equals destination port, drop them.

TCP packets with SYN and FIN bits, drop them.

TCP packets with FIN, URG and PSH bits and sequence number equals 0, drop them.

UDP

UDP packets with source port equals destination port, drop them.

Apply Cancel

The following table describes the labels in this screen.

**Table 128** DoS Prevention

LABEL	DESCRIPTION
Active	Select the check box to enable DoS prevention.
Action	Specify the action(s) and filtering criteria the Switch takes on all incoming packets.
Mac	Select the <b>If packets with source Mac address equals destination Mac address, drop them.</b> check box to discard any packets whose source MAC address and destination MAC address are the same.
IP	Select the <b>If packets with source IP address equals destination IP address, drop them.</b> check box to discard any IP packets whose source IP address and destination IP address are the same.
ICMP	select the <b>If the packets are fragmented ICMP packets, drop them.</b> check box to have the Switch discard any fragmented ICMP packets.
TCP	<p>Select the <b>Check TCP SYN packet with source port values are always 0, drop them.</b> check box to have the Switch discard any TCP SYN packets whose source port numbers are zero.</p> <p>Select the <b>TCP fragments with offset value of 1 are dropped.</b> check box to have the Switch discard any TCP fragments with a Data Offset of 1.</p> <p>Select the <b>TCP packets with control flags equals 0 and sequence number equals 0, drop them.</b> check box to have the Switch discard any TCP packets whose control (flag) bit and sequence number are 0.</p> <p>Select the <b>TCP packets with source port equals destination port, drop them.</b> check box to have the Switch discard any TCP packets whose source port and destination port are the same.</p> <p>Select the <b>TCP packets with SYN and FIN bits, drop them.</b> check box to have the Switch discard the TCP packets that contain both SYN (SYNchronize) and FIN (Finish) flags.</p> <p>Select the <b>TCP packets with FIN, URG and PSH bits and sequence number equals 0, drop them.</b> check box to have the Switch discard any TCP packets whose FIN (Finish), URG (URGent) and PSH (Push) flags bits and sequence number are 0.</p>
UDP	Select the <b>UDP packets with source port equals destination port, drop them.</b> check box to have the Switch discard any UDP packets whose source port and destination port are the same.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## PPPoE IA

This chapter describes how the Switch gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

### 32.1 PPPoE Intermediate Agent Overview

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients before forwarding them to the PPPoE server.



#### 32.1.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

**Table 129** PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2
----------------------	---------	-------	----	----

The Tag\_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag\_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the "ADSL Forum" IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.



## 32.1.2 Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

**Table 130** PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

**Table 131** PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (63 bytes)

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch puts the PPPoE client's MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

### 32.1.2.1 WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates "Ethernet".

**Table 132** PPPoE IA Circuit ID Sub-option Format: Defined in WT-101

SubOpt	Length	Value								
0x01 (1 byte)	N (1 byte)	Access Node Identifier (20 byte)	Space (1 byte)	eth (3 byte)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port No (2 byte)	: (1 byte)	VLAN ID (4 bytes)

## 32.1.3 PPPoE IA Configuration Options

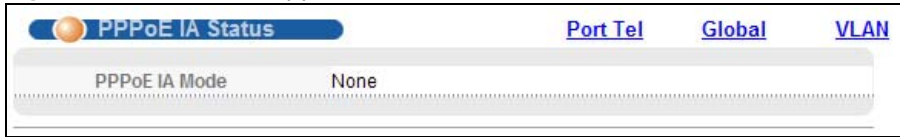
The PPPoE IA configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the PPPoE discovery packets to which you want to add subscriber line specific information on your network. Choose the configuration screen based on the following criteria:

- Global: The Switch adds the same subscriber line specific information to all PPPoE discovery packets it receives.
- VLAN: The Switch is configured on a per-VLAN basis. The Switch can be configured to add different subscriber line specific information to PPPoE discovery packets in different VLANs.

## 32.2 The PPPoE IA Status Screen

Click **Advanced Application > PPPoE IA Configuration** in the navigation panel to display the screen as shown. Use this screen to view the PPPoE Intermediate Agent status on the Switch.

**Figure 177** Advanced Application > PPPoE IA Status



The following table describes the labels in this screen.

**Table 133** Advanced Application > PPPoE IA Status

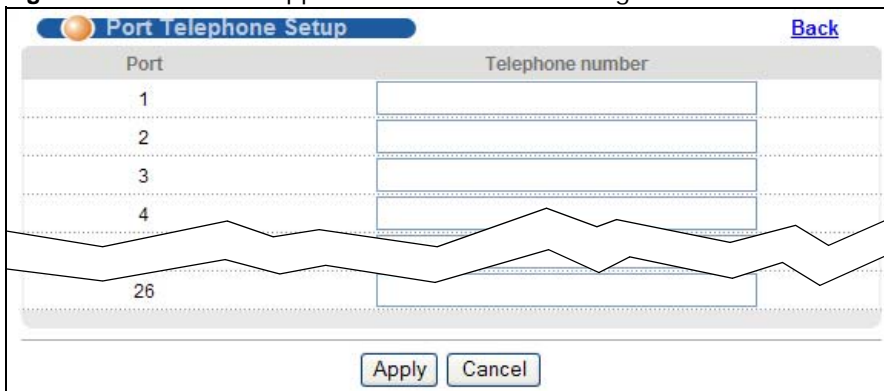
LABEL	DESCRIPTION
PPPoE IA Mode	<p>This field displays:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> if the PPPoE intermediate agent is disabled on the Switch.</li> <li>• <b>Global:</b> if the Switch is configured to add the same subscriber line specific information to all PPPoE discovery packets it receives.</li> <li>• <b>VLAN:</b> followed by a VLAN ID or multiple VLAN IDs if the Switch is configured to add subscriber line specific information to PPPoE discovery packets in specific VLAN(s).</li> </ul>

## 32.3 PPPoE IA Port Tel Configuration

Click **Advanced Application > PPPoE IA Configuration** in the navigation panel, and then click the **Port Tel** link to display the screen as shown.

Use this screen to configure telephone numbers for each port, if you want to add them into PPPoE IA option 82 tags. See more information in the **Advanced Application > PPPoE IA Configuration > Global** (see [Section 32.4 on page 291](#)) or **Advanced Application > PPPoE IA Configuration > VLAN** screen (see [Section 32.5 on page 293](#)).

**Figure 178** Advanced Application > PPPoE IA Configuration > Port Tel



The following table describes the labels in this screen.

**Table 134** Advanced Application > PPPoE IA Configuration > Port Tel

LABEL	DESCRIPTION
Port	This field shows the number of a DSL port and the VDSL port bonding group ID if the port has joined one.
Telephone number	Enter a string or digits to represent the port's telephone number. Spaces are not allowed.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 32.4 PPPoE IA Global Configuration

Click **Advanced Application > PPPoE IA Configuration** in the navigation panel, and then click the **Global** link to display the screen as shown. Use this screen to configure the global PPPoE IA settings the Switch applies to all PPPoE clients.

You can additionally configure whether to add/replace PPPoE IA option 82 tags on a per-port basis in the **Basic Setting > Port Setup** screen (see [Section 8.9 on page 82](#)).

**Figure 179** Advanced Application > PPPoE IA Configuration > Global

The screenshot shows the 'PPPoE IA Configuration' screen with the following settings:

- Active:**
- Append Circuit ID:**  Circuit ID
- Circuit ID Information:**  [Empty field],  Append Circuit ID by host name
- Tag Option:** private
- Delimiter:** none
- Append Remote ID:**  Remote ID
- Remote ID Information:**  Append Remote ID by user identifier,  Append Remote ID by port name,  Append Remote ID by user identifier + port name + port TEL
- Remote ID user identifier:** [Empty field]
- Remote ID Delimiter:** [Empty field]

Buttons: Apply, Cancel

The following table describes the labels in this screen.

**Table 135** Advanced Application > PPPoE IA Configuration > Global

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the Switch.  Note: You cannot enable this function globally if you have configured a rule for a specific VLAN on the port in the <b>Advanced Application &gt; PPPoE IA Configuration &gt; VLAN</b> screen.
Append Circuit ID	Select this option to have the Switch add the user-defined identifier string (specified in the <b>Circuit ID Information</b> field) to PADI or PADR packets from PPPoE clients.  If you leave this option unselected and do not configure any Circuit ID string (using CLI commands) on the Switch, the Switch will use its host name.
Circuit ID Information	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for any PPPoE discovery packets it forwards. Spaces are allowed.  Otherwise, select the second option to have the Switch use its host name.
Tag Option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include <b>SP</b> , <b>SV</b> , <b>PV</b> and <b>SPV</b> which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively in ASCII code. Alternatively, select <b>private</b> to have the Switch use the Agent Circuit ID old format (slot-port-VLAN) in binary. The Switch uses a zero for the slot value in the PADI and PADR packets. An example of the port number is 1 if you select <b>private</b> while it is 31 in ASCII code if you select <b>SP</b> , <b>SV</b> or <b>SPV</b> .
Delimiter	Select a delimiter to separate the Circuit ID information, slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Append Remote ID	Select <b>Remote ID</b> to have the Switch add the string (specified in the <b>Remote ID Information</b> field) to PADI or PADR packets from PPPoE clients.
Remote ID Information	Select one of the following options:  <b>Append Remote ID by user identifier:</b> to have the Switch add the specified Remote ID user identifier into the Agent Remote ID sub-option for any PPPoE discovery packets it forwards..  <b>Append Remote ID by port name:</b> to have the Switch use the name of the port on which the PPPoE discovery packets are received and add it to the PPPoE discovery packets.  <b>Append Remote ID by user identifier + port name + port TEL:</b> to have the Switch add the specified Remote ID user identifier, the port's name, and the port's telephone number into the Agent Remote ID sub-option for any PPPoE discovery packets it forwards. You can configure a telephone number for each port in the <b>Advanced Application &gt; PPPoE IA Configuration &gt; Port Tel</b> screen (see <a href="#">Section 32.3 on page 290</a> ).
Remote ID user identifier	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed.
Remote ID Delimiter	Select a delimiter to separate the Remote ID information, slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 32.5 PPPoE IA VLAN Configuration

Click **Advanced Application > PPPoE IA Configuration** in the navigation panel, and then click the **VLAN** link to display the screen as shown. Use this screen to have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-VLAN basis.

Note: This screen is not available if you have enabled PPPoE IA globally in the **Advanced Application > PPPoE IA Configuration** screen.

You can additionally configure whether to add/replace PPPoE IA option 82 tags on a per-port basis in the **Basic Setting > Port Setup** screen (see [Section 8.9 on page 82](#)).

**Figure 180** Advanced Application > PPPoE IA Configuration > VLAN

The following table describes the labels in this screen.

**Table 136** Advanced Application > PPPoE IA Configuration > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which PPPoE IA settings you configure here apply.
Append Circuit ID	Select this option to have the Switch add the user-defined identifier string (specified in the <b>Circuit ID Information</b> field) to PADI or PADR packets from PPPoE clients.  If you leave this option unselected and do not configure any Circuit ID string (using CLI commands) on the Switch, the Switch will use its host name.
Circuit ID Information	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets with the specified VLAN tag. Spaces are allowed.  Otherwise, select the second option to have the Switch use its host name.

**Table 136** Advanced Application > PPPoE IA Configuration > VLAN (continued)

LABEL	DESCRIPTION
Tag Option	Select the variables that you want the Switch to generate and add into the Agent Circuit ID sub-option for PPPoE discovery packets with the specified VLAN tag. The variable options include <b>SP</b> , <b>SV</b> , <b>PV</b> and <b>SPV</b> which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively in ASCII code. Alternatively, select <b>private</b> to have the Switch use the Agent Circuit ID old format (slot-port-VLAN) in binary. An example of the port number is 1 if you select <b>private</b> while it is 31 in ASCII code if you select <b>SP</b> , <b>SV</b> or <b>SPV</b> .
Delimiter	Select a delimiter to separate the Circuit ID information, slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Append Remote ID	Select this option to have the Switch add the user-defined identifier string (specified in the <b>Remote ID Information</b> field) to PADI or PADR packets from PPPoE clients.
Remote ID Information	<p>Select one of the following options:</p> <p><b>Append Remote ID by user identifier:</b> to have the Switch add the specified Remote ID user identifier into the Agent Remote ID sub-option for PPPoE discovery packets with the specified VLAN tag it forwards.</p> <p><b>Append Remote ID by port name:</b> to have the Switch use the name of the port on which the PPPoE discovery packets with the specified VLAN tag are received and add it to the PPPoE discovery packets.</p> <p><b>Append Remote ID by user identifier + port name + port TEL:</b> to have the Switch add the specified Remote ID user identifier, the port's name, and the port's telephone number into the Agent Remote ID sub-option for PPPoE discovery packets it forwards with the specified VLAN tag.</p>
Remote ID user identifier	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets with the specified VLAN tag received on this port. Spaces are allowed.
Remote ID Delimiter	Select a delimiter to separate the Remote ID information, slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Add	Click <b>Add</b> to insert a new VLAN-specific PPPoE IA entry to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the above fields to your previous configuration.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.
VID	This field displays the ID number of the VLAN group to which the PPPoE IA settings apply.
Tag Option	This field displays what information should be included in the Agent Circuit ID sub-option. <b>SP</b> , <b>SV</b> , <b>PV</b> and <b>SPV</b> indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively in ASCII code. Alternatively, select <b>private</b> to have the Switch use the DHCP relay option 82 old format (slot-port-VLAN) in binary. The Switch uses a zero for the slot value in the PADI and PADR packets. An example of the port number is 1 if you select <b>private</b> while it is 31 in ASCII code if you select <b>SP</b> , <b>SV</b> or <b>SPV</b> .
Delimiter	This field displays the delimiter used to separate the Circuit ID information, slot ID, port number and/or VLAN ID from each other. <b>none</b> displays if no delimiter is used.
Circuit ID	This field displays whether the Switch adds a string to the Agent Circuit ID sub-option ( <b>Enable</b> ) or not ( <b>Disable</b> ).
Remote ID	This field displays whether the Switch adds a string to the Agent Remote ID sub-option ( <b>Enable</b> ) or not ( <b>Disable</b> ).
Delete	Select the configuration entries you want to remove and click <b>Delete</b> to remove them.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 32.6 ADSL Fallback

The Switch can connect to both VDSL and ADSL CPEs and/or CPEs that have both VDSL and ADSL support. When a port is connected to an ADSL CPE and a VDSL connection cannot be established, the Switch tries using the ADSL standard(s) you specified in the **VDSL Profile > LineProfile** screen and the PVCs you configured in the **ADSL Fallback** screens for that port to make an ADSL connection.

Note: Subnet-based VLAN, protocol-based VLAN and MAC-based VLAN settings cannot apply to the port(s) on which the Switch falls back to use ADSL.

### 32.6.1 PVC Configuration

Click **Advanced Application > ADSL Fallback** in the navigation panel to display the screen as shown. Use this screen to view and configure PVCs for Ethernet over ATM (EoA) packets on individual ports.

**Figure 181** Advanced Application > ADSL Fallback > PVC

The following table describes the labels in this screen.

**Table 137** Advanced Application > ADSL Fallback > PVC

LABEL	DESCRIPTION
Active	Select the check box to enable this PVC channel.
Port	Enter the number of the DSL port for which to configure a channel.
VPI	Enter the VPI (Virtual Path Indicator) from 0 to 255 for a channel on a port. The VPI and VCI identify a channel.
VCI	Enter the VCI (Virtual Channel Indicator) from 32 to 65535 for a channel on a port.

**Table 137** Advanced Application > ADSL Fallback > PVC (continued)

LABEL	DESCRIPTION
PVID	Enter the PVID (Port VLAN ID) that the Switch assigns to untagged frames received on this channel.  This must be the VLAN ID of a VLAN that is already configured. The port that you are configuring and the uplink port must also be set to the fixed status in the VLAN.  You should also select <b>Tx Tagging</b> for the VLAN to have the Switch tag all the outgoing frames on the DSL port with this VLAN ID.
Encapsulation	Specify the encapsulation type ( <b>llc</b> or <b>vc</b> ) for this channel.
Priority	Assign a default IEEE 802.1p default priority (0 to 7). This is the priority value to add to incoming frames without a (IEEE 802.1p) priority tag.
FCS	Select <b>fcs</b> to have the Switch include the original FCS (Frame Check Sequence) in the bridged frames. Otherwise, select <b>no fcs</b> .
MVLAN	Select this option to turn on multicast VLAN for this channel.  Multicast VLAN allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
Add	Click <b>Add</b> to insert a new PVC entry to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the above fields to your previous configuration.
Index	This is the index number of the channel on this port. Click a number to edit that channel.
Active	This field displays whether the channel is enabled ( <b>Yes</b> ) or not ( <b>No</b> ).
Port	This field displays the DSL port for which this channel is configured.
VPI	This field displays the Virtual Path Identifier (VPI) for this channel.
VCI	This field displays the Virtual Circuit Identifier (VCI) for this channel.
PVID	This field displays the PVID (Port VLAN ID) to assign to untagged frames received on this channel.
Encap.	This field displays the encapsulation type ( <b>llc</b> or <b>vc</b> ) for this channel.
Priority	This field displays the priority value (0 to 7) that the Switch adds to frames that come in on this channel without a (IEEE 802.1p) priority tag.
FCS	This field displays whether the original FCS is included in the frames.
MVLAN	This field displays whether the multicast VLAN is active for this channel.
Delete	Select the entries you want to remove and click <b>Delete</b> to remove them.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.



## 32.6.2 IPPVC Configuration

Click **Advanced Application** > **ADSL Fallback** in the navigation panel, and then click the **IPPVC** link to display the screen as shown. Use this screen to view and configure IPPVCs for IPoA packets on individual ports.

**Figure 182** Advanced Application > ADSL Fallback > IPPVC

The following table describes the labels in this screen.

**Table 138** Advanced Application > ADSL Fallback > IPPVC

LABEL	DESCRIPTION
Active	Select the check box to enable this IP PVC channel.
Port	Enter the number of DSL port for which to configure a channel.
VPI	Enter the VPI (Virtual Path Indicator) from 0 to 255 for a channel on a port. The VPI and VCI identify a channel.
VCI	Enter the VCI (Virtual Channel Indicator) from 32 to 65535 for a channel on a port.
PVID	Enter the PVID (Port VLAN ID) that the Switch assigns to untagged frames received on this channel.  This must be the VLAN ID of a VLAN that is already configured. The port that you are configuring and the uplink port must also be set to the fixed status in the VLAN.  You should also select <b>Tx Tagging</b> for the VLAN to have the Switch tag all the outgoing frames on the DSL port with this VLAN ID.
Encapsulation	Specify the encapsulation type ( <b>llc</b> or <b>vc</b> ) for this channel.
Priority	Assign a default IEEE 802.1p default priority (0 to 7). This is the priority value to add to incoming frames without a (IEEE 802.1p) priority tag.
Subnet IP	Enter the subscriber's IP address to which the Switch forwards the downstream traffic on this channel.

**Table 138** Advanced Application > ADSL Fallback > IPPVC (continued)

LABEL	DESCRIPTION
Subnet Mask	Enter the subscriber's subnet mask to which the Switch forwards the downstream traffic on this channel.
Default Route	Enter the IPv4 address of the default gateway to which the Switch forwards frames received on this channel.
Add	Click <b>Add</b> to insert a new IPPVC entry to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the above fields to your previous configuration.
Index	This is the index number of the channel on this port. Click a number to edit that channel.
Active	This field displays whether the channel is enabled ( <b>Yes</b> ) or not ( <b>No</b> ).
Port	This field displays the DSL port for which this channel is configured.
VPI	This field displays the Virtual Path Identifier (VPI) for this channel.
VCI	This field displays the Virtual Circuit Identifier (VCI) for this channel.
PVID	This field displays the PVID (Port VLAN ID) to assign to untagged frames received on this channel.
Encap.	This field displays the encapsulation type ( <b>llc</b> or <b>vc</b> ) for this channel.
Priority	This field displays the priority value (0 to 7) that the Switch adds to frames that come in on this channel without a (IEEE 802.1p) priority tag.
Subnet IP	This field displays the IP address for downstream traffic on this channel.
Subnet Mask	This field displays the subnet mask for downstream traffic on this channel.
Default Route	This field displays the default gateway for this channel.
Delete	Select the entries you want to remove and click <b>Delete</b> to remove them.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.

### 32.6.3 PAEPVC Configuration

Click **Advanced Application > ADSL Fallback** in the navigation panel, and then click the **PAEPVC** link to display the screen as shown. Use this screen to view and configure PPPoA-to-PPPoE (PAE) PVCs for PAE translation on individual ports.

**Figure 183** Advanced Application > ADSL Fallback > PAEPVC

The following table describes the labels in this screen.

**Table 139** Advanced Application > ADSL Fallback > PAEPVC

LABEL	DESCRIPTION
Active	Select the check box to enable this channel.
Port	Enter the number of DSL port for which to configure a channel.
VPI	Enter the VPI (Virtual Path Indicator) from 0 to 255 for a channel on a port. The VPI and VCI identify a channel.
VCI	Enter the VCI (Virtual Channel Indicator) from 32 to 65535 for a channel on a port.
PVID	Enter the PVID (Port VLAN ID) that the Switch assigns to untagged frames received on this channel.  This must be the VLAN ID of a VLAN that is already configured. The port that you are configuring and the uplink port must also be set to the fixed status in the VLAN.  You should also select <b>Tx Tagging</b> for the VLAN to have the Switch tag all the outgoing frames on the DSL port with this VLAN ID.
Encapsulation	Specify the encapsulation type ( <b>llc</b> or <b>vc</b> ) for this channel.
Priority	Assign a default IEEE 802.1p default priority (0 to 7). This is the priority value to add to incoming frames without a (IEEE 802.1p) priority tag.
Add	Click <b>Add</b> to insert a new PAEPVC entry to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the above fields to your previous configuration.
Index	This is the index number of the channel on this port. Click a number to edit that channel.

**Table 139** Advanced Application > ADSL Fallback > PAEPVC (continued)

LABEL	DESCRIPTION
Active	This field displays whether the channel is enabled ( <b>Yes</b> ) or not ( <b>No</b> ).
Port	This field displays the DSL port for which this channel is configured.
VPI	This field displays the Virtual Path Identifier (VPI) for this channel.
VCI	This field displays the Virtual Circuit Identifier (VCI) for this channel.
PVID	This field displays the PVID (Port VLAN ID) to assign to untagged frames received on this channel.
Encap.	This field displays the encapsulation type ( <b>llc</b> or <b>vc</b> ) for this channel.
Priority	This field displays the priority value (0 to 7) that the Switch adds to frames that come in on this channel without a (IEEE 802.1p) priority tag.
Delete	Select the entries you want to remove and click <b>Delete</b> to remove them.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.
Paging	Select <b>Prev</b> or <b>Next</b> to show the previous/next screen or select a page number from the drop-down list box to display a specific page if all entries cannot be seen in one screen.

## Static Route

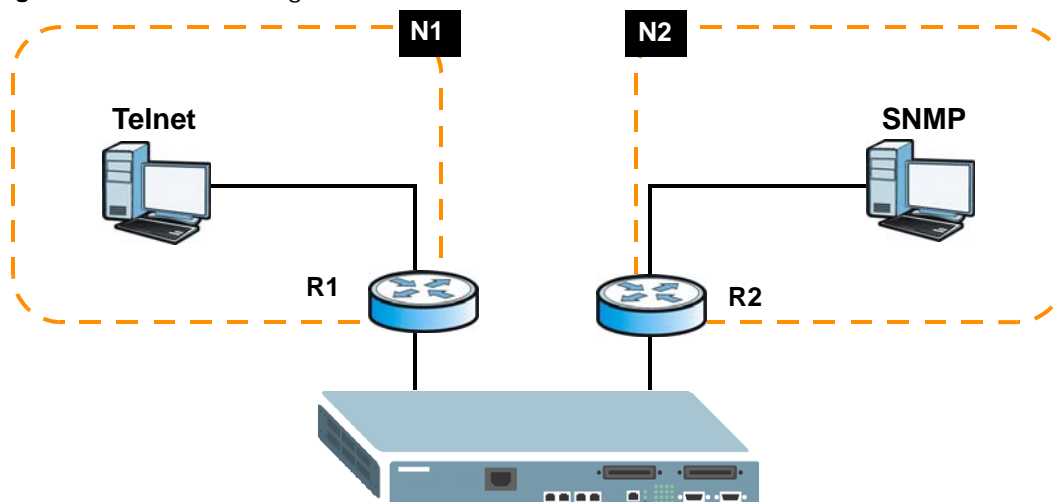
This chapter shows you how to configure static routes.

### 33.1 Static Routing Overview

The Switch uses IP for communication with management computers, for example using HTTP, Telnet, SSH, or SNMP. Use IP static routes to have the Switch respond to remote management stations that are not reachable through the default gateway. The Switch can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

This figure shows a **Telnet** session coming in from network **N1**. The Switch sends reply traffic to default gateway **R1** which routes it back to the manager's computer. The Switch needs a static route to tell it to use router **R2** to send traffic to an SNMP trap server on network **N2**.

**Figure 184** Static Routing Overview



## 33.2 Configuring Static Routing

Click **IP Application > Static Routing** in the navigation panel to display the screen as shown.

**Figure 185** IP Application > Static Routing

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	Example	172.21.1.1	255.255.0.0	192.168.1.2	2	<input type="checkbox"/>

The following table describes the related labels you use to create a static route.

**Table 140** IP Application > Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click <b>Add</b> to insert a new static route to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to reset the above fields to your previous configuration.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays <b>Yes</b> when the static route is activated and <b>NO</b> when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.

**Table 140** IP Application > Static Routing (continued)

LABEL	DESCRIPTION
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

# Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

## 34.1 DiffServ Overview

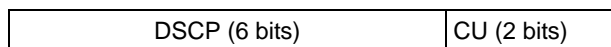
Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

### 34.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

**Figure 186** DiffServ: Differentiated Service Field



DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

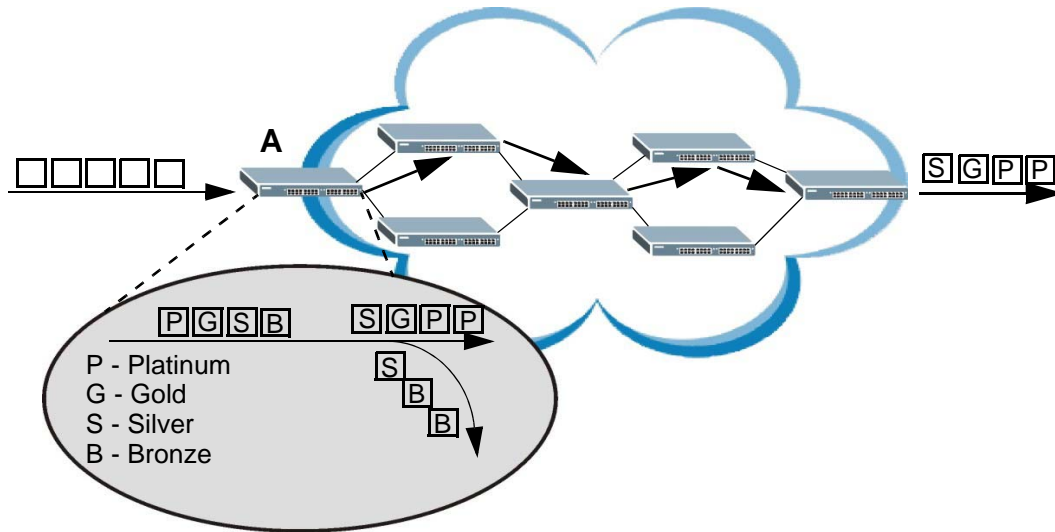
### 34.1.2 DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in [Figure 187](#)) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum, Gold, Silver, Bronze**) based on the configured marking rules. A network administrator can then apply



various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

**Figure 187** DiffServ Network



## 34.2 Two Rate Three Color Marker Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.

Two Rate Three Color Marker (TRTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

Two Rate Three Color Marker evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green. After TRTCM is configured and DiffServ is enabled the following actions are performed on the colored packets:

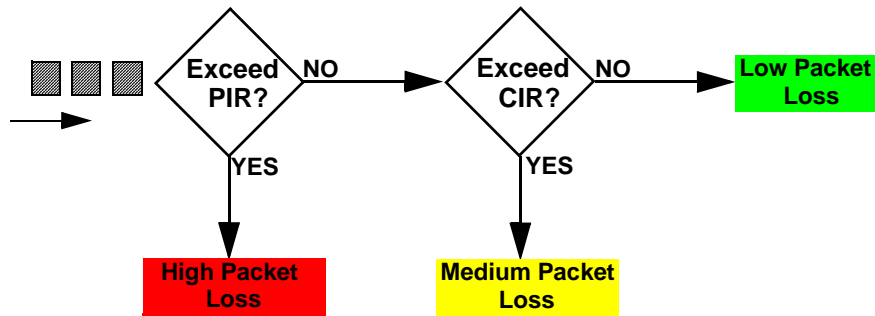
- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.
- Green (low loss priority level) packets are forwarded.

TRTCM operates in one of two modes: color-blind or color-aware. In color-blind mode, packets are marked based on evaluating against the PIR and CIR regardless of if they have previously been marked or not. In the color-aware mode, packets are marked based on both existing color and evaluation against the PIR and CIR. If the packets do not match any of colors, then the packets proceed unchanged.

### 34.2.1 TRTCM-Color-blind Mode

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

Figure 188 TRTCM-Color-blind Mode

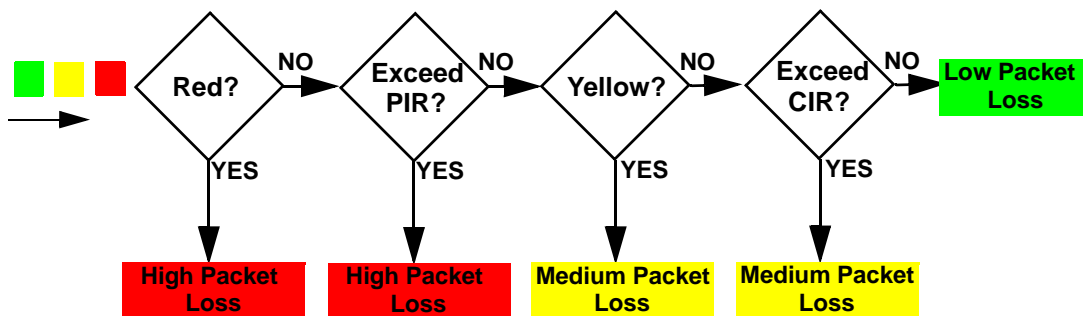


### 34.2.2 TRTCM-Color-aware Mode

In color-aware mode the evaluation of the packets uses the existing packet loss priority. TRTCM can increase a packet loss priority of a packet but it cannot decrease it. Packets that have been previously marked red or yellow can only be marked with an equal or higher packet loss priority.

Packets marked red (high packet loss priority) continue to be red without evaluation against the PIR or CIR. Packets marked yellow can only be marked red or remain yellow so they are only evaluated against the PIR. Only the packets marked green are first evaluated against the PIR and then if they don't exceed the PIR level are they evaluated against the CIR.

Figure 189 TRTCM-Color-aware Mode



## 34.3 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected port(s).

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

**Figure 190** IP Application > DiffServ

Port	Active
*	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 141** IP Application > DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  <b>Note:</b> Changes in this row are copied to all the ports as soon as you make them.
Active	Select <b>Active</b> to enable DiffServ on the port.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 34.3.1 Configuring 2-Rate 3 Color Marker Settings

Use this screen to configure TRTCM settings. Click the **2-rate 3 Color Marker** link in the **DiffServ** screen to display the screen as shown next.

Note: You cannot enable both TRTCM and Bandwidth Control at the same time.

**Figure 191** IP Application > DiffServ > 2-rate 3 Color Marker

The following table describes the labels in this screen.

**Table 142** IP Application > DiffServ > 2-rate 3 Color Marker

LABEL	DESCRIPTION
Active	Select this to activate TRTCM (Two Rate Three Color Marker) on the Switch. The Switch evaluates and marks the packets based on the TRTCM settings.  Note: You must also activate <b>DiffServ</b> on the Switch and the individual ports for the Switch to drop red (high loss priority) colored packets.
Mode	Select <b>color-blind</b> to have the Switch treat all incoming packets as uncolored. All incoming packets are evaluated against the CIR and PIR.  Select <b>color-aware</b> to treat the packets as marked by some preceding entity. Incoming packets are evaluated based on their existing color. Incoming packets that are not marked proceed through the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports.  Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.  Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to activate TRTCM on the port.
Commit Rate	Specify the Commit Information Rate (CIR) for this port.
Peak Rate	Specify the Peak Information Rate (PIR) for this port.
DSCP	Use this section to specify the DSCP values that you want to assign to packets based on the color they are marked via TRTCM.

**Table 142** IP Application > DiffServ > 2-rate 3 Color Marker (continued)

LABEL	DESCRIPTION
green	Specify the DSCP value to use for packets with low packet loss priority.
yellow	Specify the DSCP value to use for packets with medium packet loss priority.
red	Specify the DSCP value to use for packets with high packet loss priority.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 34.4 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

**Table 143** Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

### 34.4.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

**Figure 192** IP Application > DiffServ > DSCP Setting

The screenshot shows the 'DSCP Setting' screen with the following data:

DSCP Value	0	1	2	3	4	5	6	7
0-7	0	1	2	3	4	5	6	7
8-15	1	1	1	1	1	1	1	1
16-23	2	2	2	2	2	2	2	2
24-31	3	3	3	3	3	3	3	3
32-39	4	4	4	4	4	4	4	4
40-47	5	5	5	5	5	5	5	5
48-55	6	6	6	6	6	6	6	6
56-63	7	7	7	7	7	7	7	7

The following table describes the labels in this screen.

**Table 144** IP Application > DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.

**Table 144** IP Application > DiffServ > DSCP Setting (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

This chapter shows you how to configure the DHCP feature.

## 35.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the Switch as a DHCP relay agent. If you configure the Switch as a relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

### 35.1.1 DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

### 35.1.2 DHCP Configuration Options

The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global:** The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN:** The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

## 35.2 DHCP Status

Click **IP Application** > **DHCP** in the navigation panel. The **DHCP Status** screen displays.

**Figure 193** IP Application > DHCP > DHCP Status



The following table describes the labels in this screen.

**Table 145** IP Application > DHCP > DHCP Status

LABEL	DESCRIPTION
Relay Mode	This field displays: <ul style="list-style-type: none"> <li>• <b>None</b>: if the Switch is not configured as a DHCP relay agent.</li> <li>• <b>Global</b>: if the Switch is configured as a DHCP relay agent only.</li> <li>• <b>VLAN</b>: followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLAN(s).</li> </ul>

## 35.3 DHCP Port Tel

Click the **Port Tel** link in the **IP Application > DHCP** screen to open the following screen.

Use this screen to configure telephone numbers for each port, if you want to add them into DHCP option 82 tags. See more information in the **IP Application > DHCP > Global** (see [Section 35.4 on page 313](#)) or **IP Application > DHCP > VLAN** screen (see [Section 35.5 on page 318](#)).

**Figure 194** IP Application > DHCP > Port Tel

The following table describes the labels in this screen.

**Table 146** IP Application > DHCP > Port Tel

LABEL	DESCRIPTION
Port	This field shows the number of a DSL port. This field also shows the VDSL port bonding group ID if the port has joined any.
Telephone number	Enter a string or digits to represent the port's telephone number. Spaces are not allowed.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



## 35.4 DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

### 35.4.1 DHCP Relay Agent Information

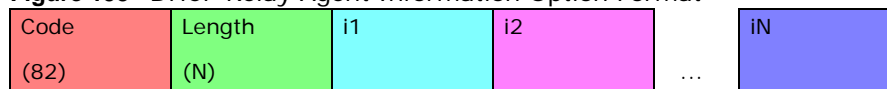
The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

### 35.4.2 DHCP Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

**Figure 195** DHCP Relay Agent Information Option Format

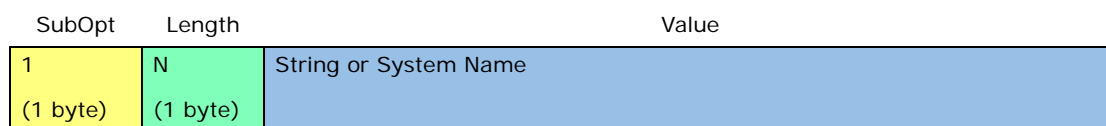


i1, i2 and iN are DHCP relay agent sub-options, which contain additional information about the DHCP client. You need to define at least one sub-option.

### 35.4.3 Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

**Figure 196** DHCP Relay Agent Circuit ID Sub-option Format



**Figure 197** DHCP Relay Agent Remote ID Sub-option Format



The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

The following describes the default DHCP relay information that the Switch sends to the DHCP server when you enable DHCP Option 82:

**Table 147** DHCP Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information (Circuit ID)	(up to 15 bytes) This is the information you want the Switch to add in the DHCP requests that it relays to a DHCP server.

You can configure the Switch to also append the remote ID to the option 82 field of DHCP requests.

### 35.4.4 Configuring DHCP Global Relay

Configure global DHCP relay in the **DHCP Relay** screen. Click **IP Application > DHCP** in the navigation panel and click the **Global** link to display the screen as shown.

**Note:** The port to which the DHCP server connects and the port(s) from which the DHCP requests come should be in the same VLAN.

You can additionally configure whether to add/replace DHCP relay option 82 tags on a per-port basis in the **Basic Setting > Port Setup** screen (see [Section 8.9 on page 82](#)).

Figure 198 IP Application &gt; DHCP &gt; Global &gt; DHCP Relay

The following table describes the labels in this screen.

Table 148 IP Application &gt; DHCP &gt; Global &gt; DHCP Relay

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.  Note: You cannot enable this function globally if you have configured a rule for a specific VLAN on the port in the <b>IP Application &gt; DHCP &gt; VLAN</b> screen.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select <b>Option 82</b> to have the Switch add information (slot number, port number and VLAN ID) and the Circuit ID and Remote ID sub-options to client DHCP requests that it relays to a DHCP server.  Select <b>Swap position of Circuit ID and Remote ID</b> to have the Switch add information (slot number, port number and VLAN ID) and the Circuit ID and Remote ID sub-option but switch their positions in client DHCP requests that it relays to a DHCP server.
Tag Option	Select which information to have the Switch generate and add into the DHCP relay option 82 Circuit ID sub-option for DHCP requests. The variable options include <b>SP</b> , <b>SV</b> , <b>PV</b> and <b>SPV</b> which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively in ASCII code. Alternatively, select <b>private</b> to have the Switch use the DHCP relay option 82 old format (slot-port-VLAN) in binary. The Switch uses a zero for the slot value in the DHCP requests. An example of the port number is 1 if you select <b>private</b> while it is 31 in ASCII code if you select <b>SP</b> , <b>SV</b> or <b>SPV</b> .

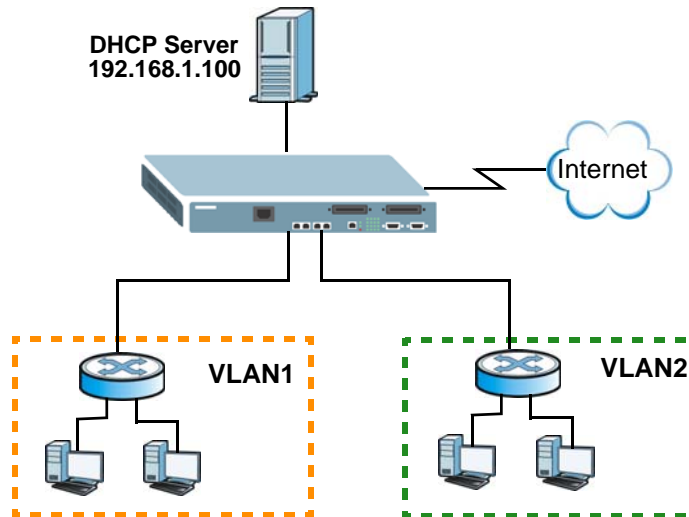
**Table 148** IP Application > DHCP > Global > DHCP Relay

LABEL	DESCRIPTION
Delimiter	Select a delimiter to separate the slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Information	Select the first option and enter a string of up to 32 ASCII or binary characters that the Switch adds into the client DHCP requests. Spaces are allowed.  Otherwise, select the second option to have the Switch use the system name you configure in the <b>General Setup</b> screen.
Relay Remote ID	Select the <b>Remote ID</b> check box to have the Switch add information configured in the <b>Remote ID Information</b> field to client DHCP requests before the Switch relays them to a DHCP server.
Remote ID Information	<b>Append Remote ID by user identifier:</b> Select this to have the Switch add the specified Remote ID user identifier into client DHCP requests received by the Switch. Spaces are allowed.  <b>Append Remote ID by port name:</b> to have the Switch use the name of the port on which the client DHCP requests are received and add it to client DHCP requests received by the Switch.  <b>Append Remote ID by user identifier + port name + port TEL:</b> to have the Switch add the specified Remote ID user identifier, the port's name, and the port's telephone number into client DHCP requests received by the Switch.
Remote ID user identifier	Enter a string of up to 63 ASCII characters that the Switch adds into client DHCP requests received on this port. Spaces are allowed.
Remote ID Delimiter	Select a delimiter to separate the slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 35.4.5 Global DHCP Relay Configuration Example

The following figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

**Figure 199** Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

**Figure 200** DHCP Relay Configuration Example

DHCP Relay		Status
Active	<input checked="" type="checkbox"/>	
Remote DHCP Server 1	<input type="text" value="192.168.1.100"/>	
Remote DHCP Server 2	<input type="text" value="0.0.0.0"/>	
Remote DHCP Server 3	<input type="text" value="0.0.0.0"/>	
Relay Agent Information	<input checked="" type="checkbox"/> Option 82	
Information	<input type="radio"/> <input type="text"/>	
	<input checked="" type="radio"/> Append Circuit ID by host name	
Relay Remote ID	<input type="checkbox"/> Remote ID	
Remote ID Information	<input checked="" type="radio"/> <input type="text"/>	
	<input type="radio"/> Append Remote ID by port name	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

## 35.5 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP** in the navigation panel, then click the **VLAN** link in the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch.

See [Section 8.7 on page 79](#) for information on how to set up management IP addresses for VLANs.

Note: This screen is not available if you have enabled DHCP Relay globally in the **IP Application** > **DHCP** > **Global** > **DHCP Relay** screen.

You can additionally configure whether to add/replace DHCP relay option 82 tags on a per-port basis in the **Basic Setting** > **Port Setup** screen (see [Section 8.9 on page 82](#)).

**Figure 201** IP Application > DHCP > VLAN

The screenshot shows the 'VLAN Setting' configuration page. It includes the following fields and options:

- VID:** Text input field.
- Remote DHCP Server 1, 2, 3:** IP address input fields, all containing '0.0.0.0'.
- Relay Agent Information:**
  - Option 82
  - Swap position of Circuit ID and Remote ID
- Tag Option:** Dropdown menu set to 'private'.
- Delimiter:** Dropdown menu set to 'none'.
- Information:**
  - (unselected)
  - Append Circuit ID by host name
- Relay Remote ID:**
  - Remote ID
- Remote ID Information:**
  - Append Remote ID by user identifier
  - Append Remote ID by port name
  - Append Remote ID by user identifier + port name + port TEL
- Remote ID user identifier:** Text input field.
- Remote ID Delimiter:** Text input field.

Buttons: Add, Cancel, Clear.

Table Header: VID, Type, DHCP Status, Delete.

Buttons: Delete, Cancel.

The following table describes the labels in this screen.

**Table 149** IP Application > DHCP > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the <b>Option 82</b> check box to have the Switch add information (slot number, port number and VLAN ID) and the Circuit ID and Remote ID sub-options to client DHCP requests that it relays to a DHCP server.
Tag Option	Select which information to have the Switch add information and the Circuit ID sub-option to client DHCP requests the Switch receives with the specified VLAN tag. The variable options include <b>SP, SV, PV</b> and <b>SPV</b> which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively in ASCII code. Alternatively, select <b>private</b> to have the Switch use the DHCP relay option 82 old format (slot-port-VLAN) in binary. The Switch uses a zero for the slot value in the DHCP requests. An example of the port number is 1 if you select <b>private</b> while it is 31 in ASCII code if you select <b>SP, SV</b> or <b>SPV</b> .
Delimiter	Select a delimiter to separate the Circuit ID information, slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Information	Select the first option and enter a string of up to 32 ASCII or binary characters that the Switch adds into the client DHCP requests. Spaces are allowed.  Otherwise, select the second option to have the Switch use the system name you configure in the <b>General Setup</b> screen.
Relay Remote ID	Select the <b>Remote ID</b> check box to have the Switch add information configured in the <b>Remote ID Information</b> field to client DHCP requests before the Switch relays them to a DHCP server.
Remote ID Information	<b>Append Remote ID by user identifier:</b> Select this to have the Switch add the specified Remote ID user identifier into client DHCP requests with the specified VLAN tag the Switch relays. Spaces are allowed.  <b>Append Remote ID by port name:</b> to have the Switch use the name of the port on which the client DHCP requests are received and add it to client DHCP requests with the specified VLAN tag the Switch relays.  <b>Append Remote ID by user identifier + port name + port TEL:</b> to have the Switch add the specified Remote ID user identifier, the port's name, and the port's telephone number into client DHCP requests the Switch relays with the specified VLAN tag.
Remote ID user identifier	Enter a string of up to 63 ASCII characters that the Switch adds into client DHCP requests with the specified VLAN tag the Switch relays. Spaces are allowed.
Remote ID Delimiter	Select a delimiter to separate the slot ID, port number and/or VLAN ID from each other. You can use a pound key ( <b>#</b> ), semi-colon ( <b>;</b> ), period ( <b>.</b> ), comma ( <b>,</b> ), forward slash ( <b>/</b> ) or <b>space</b> . Select <b>none</b> to not use any delimiter.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Clear	Click this to clear the fields above.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays the DHCP mode ( <b>Relay</b> ).
DHCP Status	For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click <b>Delete</b> to remove them.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

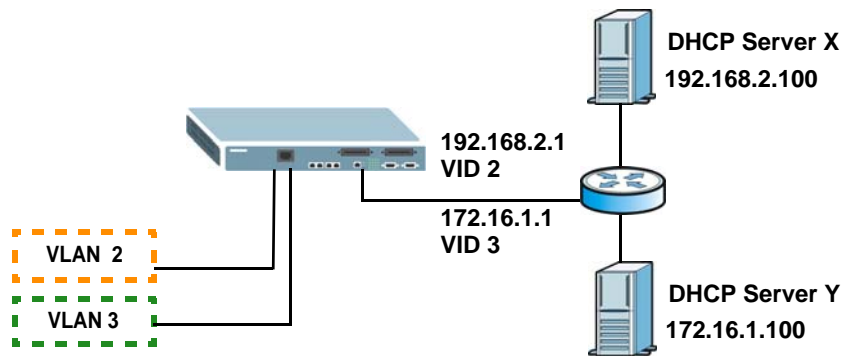
### 35.5.1 Example: DHCP Relay for Two VLANs

The following example displays two VLANs (VIDs **2** and **3**) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN **2**) to DHCP server **X** with an IP address of 192.168.2.100. Requests from the academic buildings (VLAN **3**) are sent to DHCP server **Y** with an IP address of 172.16.1.100.

Note: The port to which the DHCP server connects and the port(s) from which the DHCP requests come should be in the same VLAN.

Note: To let the Switch discover DHCP servers **X** and **Y** using ARP, you must create an IP domain and management IP address for VLANs **2** and **3**.

**Figure 202** DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

**Figure 203** DHCP Relay for Two VLANs Configuration Example

The screenshot shows the 'VLAN Setting' configuration screen. The 'VID' field is set to 3. The 'Remote DHCP Server 1' field is set to 172.16.1.100. The 'Remote DHCP Server 2' and 'Remote DHCP Server 3' fields are set to 0.0.0.0. The 'Relay Agent Information' section has 'Option 82' checked. The 'Information' section has 'Append Circuit ID by host name' selected. The 'Relay Remote ID' section has 'Remote ID' unchecked. The 'Remote ID Information' section has 'Append Remote ID by port name' selected. Below the configuration fields are 'Add', 'Cancel', and 'Clear' buttons. At the bottom, there is a table with one entry for VID 2, Type Relay, and DHCP Status 192.168.2.100. Below the table are 'Delete' and 'Cancel' buttons.

VID	Type	DHCP Status	Delete
2	Relay	192.168.2.100	<input type="checkbox"/>



## 35.6 DHCPv6 LDRA

Click **IP Application > DHCPv6 LDRA** in the navigation panel to display the screen shown next. Use this screen to add information to client DHCPv6 requests from different VLANs before forwarding the requests to the DHCPv6 server. This information helps in authenticating the source of the requests. You can also specify additional information for the system to add to the DHCPv6 requests that it relays to the DHCPv6 server.

**Figure 204** DHCPv6 LDRA

**LDRA Setup**
[DHCPv6 Counter](#) [Snooping Configure](#)

**LDRA Setup**

VLAN ID

LDRA  Enable

Option 18(Interface-ID)  Enable

Option 37(Remote-ID)  Enable

Port	Control	Untrust
1	<input checked="" type="radio"/> Client-facing <input type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
2	<input checked="" type="radio"/> Client-facing <input type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
3	<input checked="" type="radio"/> Client-facing <input type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
4	<input checked="" type="radio"/> Client-facing <input type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
22-B01*	<input checked="" type="radio"/> Client-facing <input type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
23-B01	<input checked="" type="radio"/> Client-facing <input type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
24	<input checked="" type="radio"/> Client-facing <input type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
25	<input type="radio"/> Client-facing <input checked="" type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client
26	<input type="radio"/> Client-facing <input checked="" type="radio"/> Network-facing	<input type="radio"/> Forbidden <input type="checkbox"/> Untrust Client

VID	LDRA	Option 18	Option 37	Option 18 Info	Option 37 Info	Delete
<a href="#">100</a>	Enabled	Enabled	Disabled	VES1724-56		<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 150** DHCPv6 LDRA

LABEL	DESCRIPTION
VLAN ID	Enter a VLAN ID (between 1 and 4094) to be served with DHCPv6 LDRA. Make sure the VLAN ID exists before you configure a DHCPv6 LDRA entry.
LDRA	Lightweight DHCPv6 Relay Agent (LDRA) adds information to client DHCPv6 requests before forwarding them to the DHCPv6 server. Select <b>Enable</b> to add information such as this system's host name and subscriber port from which the request was received. Clear <b>Enable</b> to have the system forward DHCPv6 requests for this VLAN without adding information.
Option18 (Interface ID)	Option 18 is required for LDRA. Select <b>Enable</b> and specify the Interface ID information to add to the client DHCPv6 requests forwarded for this VLAN to identify the interface which received the client message. For example, use "%hname%%pid%svlan" to add this system's host name, subscriber port ID, and SVLAN ID from which the request was received.
Option37 (Remote ID)	<p>The required option 18 can only add up to 127 characters of information about the DHCPv6 requests forwarded for this VLAN. Use option 37 if you need to add extra information beyond what you configure for option 18.</p> <p>Option 37 (Remote ID Info) is the DHCPv6 equivalent for the Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Relay Agent Option's Remote-ID suboption.</p> <p>Select <b>Enable</b> and specify additional information to add to the client DHCPv6 requests forwarded for this VLAN. For example, use "%hname%mac" to add this system's host name and the MAC address of the client that sent the request.</p>
Port	This field displays the index number of a port on the Switch. This field also displays the port bonding group ID if the port has joined a group, for example, 22-B01 where B01 is port 22's group ID. A star (*) displays next to the group ID if the port is the main port in that group.

**Table 150** DHCPv6 LDRA (continued)

LABEL	DESCRIPTION
Control	<p>Select the role for each port on the Switch.</p> <p><b>Client-facing:</b> this is an interface on a DHCPv6 relay agent that forwards traffic towards the DHCPv6 client. A client-facing interface on this Switch can be a DSL port or an Ethernet port which connects another LDRA-enabled Switch or DSLAM.</p> <p><b>Network-facing:</b> this is an interface on a DHCPv6 relay agent that forwards traffic towards the DHCPv6 server. A network-facing interface on this Switch should be an Ethernet port.</p> <p><b>Forbidden:</b> select this to have the Switch not add any information to DHCPv6 requests it receives. The Switch drops all DHCPv6 requests for a VLAN if this is set and DHCPv6 LDRA is enabled on the VLAN.</p> <p>A client-facing port only accepts the following types of DHCPv6 messages and drops the others.</p> <p>SOLICIT(1), REQUEST(3), CONFIRM(4), RENEW(5), REBIND(6), RELEASE(8), DECLINE(9), INFORMATION-REQUEST(11), RELAY-FORW(12)</p> <p>A network-facing port only accepts the following types of DHCPv6 messages and drops the others.</p> <p>RELAY-REPLY(13), ADVERTISE(2), REPLY(7), RECONFIGURE(10)</p> <p><b>Note:</b> You must configure at least one network-facing port on the Switch.</p> <p><b>Note:</b> Use the network-facing role for the Ethernet port you use as the uplink port to connect towards the DHCPv6 server. Use the client-facing role for an Ethernet port on the Switch that you use to connect a subtended (daisy-chained) LDRA-enabled Switch or DSLAM. Use the network-facing role for the uplink port on the subtended Switch or DSLAM. If an Ethernet port (ex. port 26) on the Switch is the uplink port that connects to the DHCPv6 server and you connect port 25 to another LDRA-enabled Switch or DSLAM, you must set port 26's role to network-facing and port 25's to client-facing. The port role on the other end of port 25 must be set to network-facing.</p>
Untrust	Select <b>Untrust Client</b> to have the Switch drop all RELAY-FORW(12) type DHCPv6 messages.
Add	Click <b>Add</b> to create a new DHCPv6 LDRA entry.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
VID	This is the ID number of the VLAN group. Click the link to modify the LDRA entry's settings.
LDRA	This field displays whether LDRA is enabled or not on this VLAN.
Option18	This field displays whether or not the system adds option 18 (Interface ID Info) to the client DHCPv6 requests forwarded for this VLAN.
Option37	This field displays whether or not the system adds option 37 (Remote ID Info) to the client DHCPv6 requests forwarded for this VLAN.
Option18 (Interface ID) Info	This field displays the option 18 (Interface ID) information to add to the client DHCPv6 requests forwarded for this VLAN to identify the interface which received the client message.
Option37 (Remote ID) Info	This field displays the option 37 (Remote ID) information to add to the client DHCPv6 requests forwarded for this VLAN.
Select	Select an entry's <b>Delete</b> check box and click the <b>Delete</b> button to remove the entry or click <b>Modify</b> to edit the entry.
Delete	Click <b>Delete</b> to remove the selected entries.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 35.6.1 DHCPv6 Counter

Click **DHCPv6 Counter** link in the **IP Application > DHCPv6 LDRA** screen to display the screen shown next. Use this screen to view DHCPv6 packet statistics.

**Figure 205** DHCPv6 Counter

The following table describes the labels in this screen.

**Table 151** DHCPv6 Counter

LABEL	DESCRIPTION
Reload	Select a port from the drop-down list box and click <b>Reload</b> to display the counters for the port.  Note: For ports in a bonding group, the counter information on this screen is only available for the main port. A star (*) displays next to the bonding group ID if the port is the main port in that group.
Port No.	This field displays the index number of the selected port.
Message Type	This field displays all possible types of DHCPv6 messages.
Counter	This field displays the number of each message type the went through the port.

## 35.6.2 Snooping Configure

Click the **Snooping Configure** link in the **IP Application > DHCPv6 LDRA** screen to display the screen shown next. Use this screen to configure an acceptable rate for receiving DHCPv6 packets on each port. A port dropped additional DHCP packets after the receiving rate reaches the

configured number.

**Figure 206** Snooping Configure

Port	Rate (pps)
*	<input type="text"/>
1	<input type="text" value="0"/>
2	<input type="text" value="0"/>
3	<input type="text" value="0"/>
4	<input type="text" value="0"/>
22-B01*	<input type="text" value="0"/>
23-B01	<input type="text" value="0"/>
24	<input type="text" value="0"/>
25	<input type="text" value="0"/>
26	<input type="text" value="0"/>

The following table describes the labels in this screen.

**Table 152** Snooping Configure

LABEL	DESCRIPTION
Port	This field displays the index number of a port on the Switch. This field also displays the port bonding group ID if the port has joined any, for example, 22-B01 where B01 is port 22's group ID.
Rate (pps)	Enter the maximum number of DHCPv6 packets the port can receive in a second.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



## Maintenance

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

### 36.1 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management > Maintenance** in the navigation panel to open the following screen.

**Figure 207** Management > Maintenance



The following table describes the labels in this screen.

**Table 153** Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration ( <b>Configuration 1</b> or <b>Configuration 2</b> ) is currently operating on the Switch.
Firmware Upgrade	Click <b>Click Here</b> to go to the <b>Firmware Upgrade</b> screen.
Restore Configuration	Click <b>Click Here</b> to go to the <b>Restore Configuration</b> screen.
Backup Configuration	Click <b>Click Here</b> to go to the <b>Backup Configuration</b> screen.
Load Factory Default	Click <b>Click Here</b> to reset the configuration to the factory default settings. If you want to reset all settings to factory defaults but keep current IP settings, click <b>Without Management IP</b> instead.
Save Configuration	Click <b>Config 1</b> to save the current configuration settings to <b>Configuration 1</b> on the Switch. Click <b>Config 2</b> to save the current configuration settings to <b>Configuration 2</b> on the Switch.
Reboot System	Click <b>Config 1</b> to reboot the system and load <b>Configuration 1</b> on the Switch. Click <b>Config 2</b> to reboot the system and load <b>Configuration 2</b> on the Switch.  Note: Make sure to click the <b>Save</b> button in any screen to save your settings to the current configuration on the Switch.

## 36.2 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Firmware is uploaded to the current image. See [Section 36.8 on page 331](#) for more information about images and uploading firmware to a different image.

**Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.**

### 36.2.1 Dual Firmware Image

You can store up to two firmware files (of the same device model) on the switch. Only one firmware is used at a time. This allows immediate rollback on system bootup in case the current firmware is corrupt. By default, the switch uses firmware ras-0 while the second firmware file is named ras-1.

- You can select which firmware to use during system startup using the `boot image <1|2>` command (where 1 is ras-0 and 2 is ras-1).
- To specify whether to save a new firmware to ras-0 or ras-1 on the switch, perform firmware upgrade using the FTP commands (refer to [Section 36.8 on page 331](#)).
- If the switch fails to start from the exiting firmware, access the device console port and use the `ATGI` command to set the switch to use the second firmware to start up.

Click **Management** > **Maintenance** > **Firmware Upgrade** to view the screen as shown next.

Note: Firmware upgrade using the web configurator saves the new firmware to ras-0.

**Figure 208** Management > Maintenance > Firmware Upgrade

The screenshot shows a web interface for firmware upgrade. At the top, there is a navigation bar with 'Firmware Upgrade' and 'Maintenance'. Below the navigation bar, there is a heading: 'To upgrade the internal switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.' Underneath the heading, there is a 'File Path' text input field, a 'Browse...' button, and a checked 'Rebooting' checkbox. At the bottom of the form, there is an 'Upgrade' button.

Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Select the **Rebooting** check box if you want to reboot the Switch and apply the new firmware immediately. (Firmware upgrades are only applied after a reboot.) Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.



### 36.2.1.1 Checking Firmware Version via the Console Port

You can check which firmware version the device uses during system startup through the console port.

```

Bootbase Version: V56Fanless | 10/23/2012 11:00:25
RAM: Size = 131072 Kbytes
DRAM POST: Testing: 23488K
OK
FLASH: AMD 128M *1

ZyNOS Version: V56_Fanless130626 | 06/26/2013 10:21:50

Press any key to enter debug mode within 3 seconds.
.....

```

After the system successfully boots up, use the `show system-information` command to check which firmware image file the Switch currently uses (in the **Current Boot Image** field). The following figure shows an example in which the Switch is set to use the second firmware image (`ras-1`).

```

VES1724-56# show system-information

Product Model       : VES1724-56
System Name        : VES1724-56
System Contact     :
System Location    :
System up Time     : 0:01:52 (2bde ticks)
Ethernet Address   : cc:5d:4e:00:00:02
Bootbase Version   : V56Fanless | 10/23/2012
ZyNOS F/W Version  : V56_Fanless130626 | 06/26/2013
Config Boot Image  : 1
Current Boot Image : 2
Power Module       : AC
1st F/W Version    : V56_Fanless130626 | 06/26/2013
2nd F/W Version    : V1015GPIO3 | 10/15/2012
sysname#

```

## 36.3 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

**Figure 209** Management > Maintenance > Restore Configuration

The screenshot shows a web-based interface for restoring a configuration file. At the top, there is a blue header with a globe icon and the text 'Restore Configuration', and a 'Maintenance' tab on the right. Below the header, there is a text box with instructions: 'To restore the device's configuration from a file, browse the location of the configuration file and click Restore button.' Underneath the instructions is a 'File Path' label followed by an empty text input field and a 'Browse...' button. At the bottom of the form, there is a 'Restore' button.

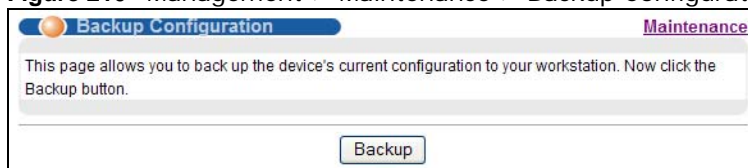
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

## 36.4 Backup a Configuration File

Backing up your Switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

**Figure 210** Management > Maintenance > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

- 1 Click **Backup** to display the current Switch configurations in a text file.
- 2 Click **File > Save As...** and choose a location to save the configuration file to your computer.

## 36.5 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Default** to clear all Switch configuration information you configured and return to the factory defaults. If you want to reset all settings to factory defaults but keep current IP settings, click **Without Management IP** instead.

**Figure 211** Load Factory Default: Confirmation



- 2 Click **OK** to confirm the action.
- 3 In the Web Configurator, click the **Save** button in the top of the screen to make the changes take effect. If you click the **Click Here** button and want to access the Switch Web Configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

## 36.6 Save Configuration

In the **Management > Maintenance** screen, click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

## 36.7 Reboot System

Reboot **System** allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

- 1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

**Figure 212** Reboot System: Confirmation



- 2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

## 36.8 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

### 36.8.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension.

**Table 154** Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.cfg	This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras-0 ras-1	*.bin	This is the generic name for the ZyNOS firmware on the Switch. ras-0 is image 1; ras-1 is image 2.

You can store up to two images, or firmware files of the same device model, on the Switch. Only one image is used at a time.

- Run the `boot image <1|2>` command to specify which image is updated when firmware is loaded using the Web Configurator and to specify which image is loaded when the Switch starts up.
- You can also use FTP commands to upload firmware to any image.

The Switch supports dual firmware images, `ras-0` and `ras-1`. You can switch from one to the other by using the `boot image <index>` command, where `<index>` is 1 (`ras-0`) or 2 (`ras-1`). See the CLI Reference Guide for more information about using commands. The system does not reboot after it switches from one image to the other.

### 36.8.1.1 Example FTP Commands

```
ftp> put firmware.bin ras-0
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config", "ras-0", and "ras-1". Be sure you keep unaltered copies of all files for later use.

**Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.**

### 36.8.2 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter `open`, followed by a space and the IP address of your Switch.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "1234").

- 5 Enter `bin` to set transfer mode to binary.
- 6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras-0` transfers the firmware on your computer (`firmware.bin`) to the Switch and renames it to "ras-0". Similarly, `put config.cfg config` transfers the configuration file on your computer (`config.cfg`) to the Switch and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to "config.cfg". See [Table 154 on page 332](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

### 36.8.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous.  This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.  Normal.  The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

### 36.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

## Access Control

This chapter describes how to control access to the Switch.

### 37.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

**Table 155** Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the CLI Reference Guide for more information on disabling multi-login.

### 37.2 The Access Control Main Screen

Click **Management** > **Access Control** in the navigation panel to display the main screen as shown.

**Figure 213** Management > Access Control

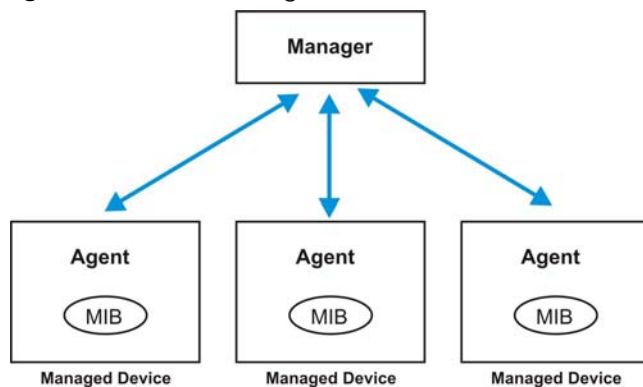


### 37.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version one (SNMPv1), SNMP version 2c or

SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

**Figure 214** SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the Switch). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

**Table 156** SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

### 37.3.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

## 37.3.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1493 Bridge MIBs
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- RFC3728 VDSL line MIB
- RFC5650 VDSL2 line MIB
- RFC2662 ADSL line MIB
- RFC3440 ADSL extension line MIB
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP
- xDSL2 MIB draft version 6.
- CFM 802.1ag draft version 8.0
- ZyXEL private MIBs
- IPv6 standard MIB:
  - IP-FORWARD-MIB (RFC 4292)
  - IP-MIB (RFC 4293)
  - IPv6-TCP-MIB (RFC 2452)
  - TCP-MIB (RFC 4022)
  - UDP-MIB (RFC 4113)
  - INET-ADDRESS-MIB (RFC 2851)

## 37.3.3 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with “**1.3.6.1.4.1.890.1.5.12.46**” is defined in private MIBs. Otherwise, it is a standard MIB OID.

**Table 157** SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.



**Table 157** SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
fanspeed	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when the fan speed returns to the normal operating range.
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when the voltage returns to the normal operating range.
rxCRC	rxCRCEventON	1.3.6.1.4.1.890.1.5.12.46.27.2.1	This trap is sent when the downlink port receives more than 10000 rxCRC messages within 10 seconds.
	rxCRCEventClear	1.3.6.1.4.1.890.1.5.12.46.27.2.2	This trap is sent when the amount of rxCRC messages the downlink port receives within 10 seconds returns to the normal number (less than 10000).
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when the Switch automatically resets.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when the Switch resets by an administrator through a management interface.
	RebootEvent	1.3.6.1.4.1.890.1.5.0.1	This trap is sent when the Switch reboots by an administrator through a management interface.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when loopguard shuts down a port.
externalalarm	ExternalAlarmEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when the external alarm is received.
	ExternalAlarmEventClear	1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when the external alarm stops sending an alert.
LPR	LPREventOn	1.3.6.1.4.1.890.1.5.12.46.27.2.1	This trap is sent when the system loses power.

**Table 157** SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
HRinformati on	cpualarmEventOn	1.3.6.1.4.1.890.1.5.12.46.27.2.1	This trap is sent when the amount of CPU usage goes over the CPU utilization threshold.
	cpualarmEventClear	1.3.6.1.4.1.890.1.5.12.46.27.2.2	This trap is sent when the amount of CPU usage goes below the CPU utilization threshold.
	packetalarmEventOn	1.3.6.1.4.1.890.1.5.12.46.27.2.1	This trap is sent when the amount of packet buffer usage goes over the packet utilization threshold.
	packetalarmEventClear	1.3.6.1.4.1.890.1.5.12.46.27.2.2	This trap is sent when the amount of packet buffer usage goes below the packet utilization threshold.
	memoryalarmEventOn	1.3.6.1.4.1.890.1.5.12.46.27.2.1	This trap is sent when the amount of memory usage goes over the memory utilization threshold.
	memoryalarmEventClear	1.3.6.1.4.1.890.1.5.12.46.27.2.2	This trap is sent when the amount of memory usage goes below the memory utilization threshold.

**Table 158** SNMP Interface Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when the Ethernet link is down.
autonegotiatio n	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when an Ethernet interface auto-negotiates with the peer Ethernet interface.
SFP	DdmiTemperatureAlarmEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.7.2.1	This trap is sent when a transceiver's temperature goes over the "high alarm" threshold.
	DdmiTxPowerAlarmEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.7.2.1	This trap is sent when a transceiver's transmitted optical power goes over the "high alarm" threshold.

**Table 158** SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
	DdmiRxPowerAlarmEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's received optical power goes over the "high alarm" threshold.
	DdmiVoltageAlarmEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's voltage goes over the "high alarm" threshold.
	DdmiTxBiasAlarmEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's laser bias current goes over the "high alarm" threshold.
	DdmiTemperatureWarnEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's temperature goes over the "high warning" threshold.
	DdmiTxPowerWarnEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's transmitted optical power goes over the "high warning" threshold.
	DdmiRxPowerWarnEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's received optical power goes over the "high warning" threshold.
	DdmiVoltageWarnEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's voltage goes over the "high warning" threshold.
	DdmiTxBiasWarnEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.1	This trap is sent when a transceiver's laser bias current goes over the "high warning" threshold.
	DdmiTemperatureAlarmEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.2	This trap is sent when a transceiver's temperature falls down below the high alarm threshold and is back to the normal range.
	DdmiTxPowerAlarmEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.2	This trap is sent when a transceiver's transmitted optical power falls down below the high alarm threshold and is back to the normal range.
	DdmiRxPowerAlarmEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.2	This trap is sent when a transceiver's received optical power falls down below the high alarm threshold and is back to the normal range.
	DdmiVoltageAlarmEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.2	This trap is sent when a transceiver's voltage falls down below the high alarm threshold and is back to the normal range.
	DdmiTxBiasAlarmEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.2	This trap is sent when a transceiver's laser bias current falls down below the high alarm threshold and is back to the normal range.
	DdmiTemperatureWarnEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.2	This trap is sent when a transceiver's temperature falls down below the high warning threshold and is back to the normal range.
	DdmiTxPowerWarnEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.2 7.2.2	This trap is sent when a transceiver's transmitted optical power falls down below the high warning threshold and is back to the normal range.

**Table 158** SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
	DdmiRxPowerWarnEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.27.2.2	This trap is sent when a transceiver's received optical power falls down below the high warning threshold and is back to the normal range.
	DdmiVoltageWarnEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.27.2.2	This trap is sent when a transceiver's voltage falls down below the high warning threshold and is back to the normal range.
	DdmiTxBiasWarnEventCleared	1.3.6.1.4.1.890.1.5.12.46.45.27.2.2	This trap is sent when a transceiver's laser bias current falls down below the high warning threshold and is back to the normal range.

**Table 159** AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.12.46.45.27.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.12.46.45.27.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.12.46.45.27.2	This trap is sent when the RADIUS server can be reached.
accounting	accountingEventOn	1.3.6.1.4.1.890.1.5.12.46.27.27.1	This trap is sent when a user fails to log into the Web Configurator or the CLI command mode.

**Table 160** SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MRSTPNewRoot	1.3.6.1.4.1.890.1.5.12.46.45.36.2.1	This trap is sent when the MRSTP root switch changes.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.12.46.45.107.70.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MRSTPTopologyChange	1.3.6.1.4.1.890.1.5.12.46.45.36.2.2	This trap is sent when the MRSTP topology changes.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.12.46.45.107.70.2	This trap is sent when the MSTP root switch changes.

**Table 160** SNMP Switch Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.12.46.45.2.1	This trap is sent when more than 99% of the MAC table is used.
	MacTableFullEventClear	or 1.3.6.1.4.1.890.1.5.12.46.45.2.2	This trap is sent when less than 95% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.

**Table 161** SNMP VDSL Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
alarmprofile	xdsl2LinePerfFECSThreshXtuc	1.3.6.1.2.1.10.251.0.1	This trap is sent when the Switch detects that the number of FEC seconds exceeds the threshold.
	xdsl2LinePerfFECSThreshXtur	1.3.6.1.2.1.10.251.0.2	This trap is sent when the number of FEC seconds in CPE side exceeds the threshold.
	xdsl2LinePerfESThreshXtuc	1.3.6.1.2.1.10.251.0.3	This trap is sent when the Switch detects that the number of errored seconds exceeds the threshold.
	xdsl2LinePerfESThreshXtur	1.3.6.1.2.1.10.251.0.4	This trap is sent when the number of errored seconds in CPE side exceeds the threshold.
	xdsl2LinePerfSESThreshXtuc	1.3.6.1.2.1.10.251.0.5	This trap is sent when the Switch detects that the number of severely errored seconds exceeds the threshold.
	xdsl2LinePerfSESThreshXtur	1.3.6.1.2.1.10.251.0.6	This trap is sent when the number of severely errored seconds in CPE side exceeds the threshold.
	xdsl2LinePerfLOSSThreshXtuc	1.3.6.1.2.1.10.251.0.7	This trap is sent when the Switch detects that the number of LOS seconds exceeds the threshold.
	xdsl2LinePerfLOSSThreshXtur	1.3.6.1.2.1.10.251.0.8	This trap is sent when the number of LOS seconds in CPE side exceeds the threshold.
	xdsl2LinePerfUASThreshXtuc	1.3.6.1.2.1.10.251.0.9	This trap is sent when the Switch detects that the number of unavailable seconds exceeds the threshold.
	xdsl2LinePerfUASThreshXtur	1.3.6.1.2.1.10.251.0.10	This trap is sent when the number of unavailable seconds in CPE side exceeds the threshold.
	xdsl2LinePerfCodingViolationsThreshXtuc	1.3.6.1.2.1.10.251.0.11	This trap is sent when the Switch detects that the number of coding violations exceeds the threshold..
	xdsl2LinePerfCodingViolationsThreshXtur	1.3.6.1.2.1.10.251.0.12	This trap is sent when the number of coding violations in CPE side exceeds the threshold.
	xdsl2LinePerfCorrectedThreshXtuc	1.3.6.1.2.1.10.251.0.13	This trap is sent when the Switch detects that the number of corrected blocks (FEC events) exceeds the threshold.

**Table 161** SNMP VDSL Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
	xdsl2LinePerfCorrectedThreshXtur	1.3.6.1.2.1.10.251.0.14	This trap is sent when the number of corrected blocks (FEC events) in CPE side exceeds the threshold.
	xdsl2LinePerfFailedFullInitThresh	1.3.6.1.2.1.10.251.0.15	This trap is sent when the number of full initialization failure times for an ADSL/ADSL2/ADSL2+ line exceeds the threshold.
	xdsl2LinePerfFailedShortInitThresh	1.3.6.1.2.1.10.251.0.16	This trap is sent when the number of short initialization failure times for an ADSL/ADSL2/ADSL2+ line exceeds the threshold.
others	xdsl2LineStatusChangeXtur	1.3.6.1.2.1.10.251.0.17	This trap is sent when the Switch detects that a DSL line's status changes.
	xdsl2LineStatusChangeXtur	1.3.6.1.2.1.10.251.0.18	This trap is sent when a DSL line's status changes at the CPE end.

### 37.3.4 Configuring SNMP

Click **Management > Access Control > SNMP** to view the screen as shown. Use this screen to configure your SNMP settings.

**Figure 215** Management > Access Control > SNMP

The screenshot shows the SNMP configuration page with three main sections:

- General Setting:** Includes dropdown for Version (v2c), and text input fields for Get Community, Set Community, and Trap Community, all set to 'public'.
- Trap Destination:** A table with columns for Version, IP, Port, and Username. It contains four rows, each with Version set to v2c, IP set to 0.0.0.0, and Port set to 162.
- User Information:** A table with columns for Index, Username, Security Level, Authentication, and Privacy. It contains one row with Index 1, Username 'admin', Security Level 'noauth', Authentication 'MD5', and Privacy 'DES'.

Buttons for 'Apply' and 'Cancel' are located at the bottom of the form.

The following table describes the labels in this screen.

**Table 162** Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c ( <b>v2c</b> ), SNMP version 3 ( <b>v3</b> ) or both ( <b>v3v2c</b> ).  Note: SNMP version 2c is backwards compatible with SNMP version 1.

**Table 162** Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Get Community	Enter the <b>Get Community</b> string, which is the password for the incoming Get- and GetNext- requests from the management station.  The <b>Get Community</b> string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the <b>Set Community</b> , which is the password for incoming Set- requests from the management station.  The <b>Set Community</b> string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the <b>Trap Community</b> string, which is the password sent with each trap to the SNMP manager.  The <b>Trap Community</b> string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IPv4 or IPv6 addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap.  <b>Note:</b> This username must match an existing account on the Switch (configured in the <b>Management &gt; Access Control &gt; Logins</b> screen).
User Information	Use this section to configure users for authentication with managers using SNMP v3.  <b>Note:</b> Use the username and password of the login accounts you specify in this section to create accounts on the SNMP v3 manager.
Index	This is a read-only number identifying a login account on the Switch.
Username	This field displays the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: <ul style="list-style-type: none"> <li>• <b>noauth:</b> to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level.</li> <li>• <b>auth:</b> to implement an authentication algorithm for SNMP messages sent by this user.</li> <li>• <b>priv:</b> to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level.</li> </ul> <b>Note:</b> The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. <b>MD5</b> (Message Digest 5) and <b>SHA</b> (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. <b>SHA</b> authentication is generally considered stronger than <b>MD5</b> , but is slower.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>DES</b> - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.</li> <li>• <b>AES</b> - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.</li> </ul>
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 37.3.5 Configuring SNMP Trap Group

Click **Management > Access Control > SNMP > Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

**Figure 216** Management > Access Control > SNMP > Trap Group

Type	Options
System <input type="checkbox"/> *	<input type="checkbox"/> coldstart <input type="checkbox"/> warmstart <input type="checkbox"/> fanspeed <input type="checkbox"/> temperature <input type="checkbox"/> voltage <input type="checkbox"/> rxCRC <input type="checkbox"/> reset <input type="checkbox"/> loopguard <input type="checkbox"/> externalalarm <input type="checkbox"/> LPR <input type="checkbox"/> HWinformation
Interface <input type="checkbox"/> *	<input type="checkbox"/> linkup <input type="checkbox"/> linkdown <input type="checkbox"/> autonegotiation <input type="checkbox"/> SFP
AAA <input type="checkbox"/> *	<input type="checkbox"/> authentication <input type="checkbox"/> accounting
Switch <input type="checkbox"/> *	<input type="checkbox"/> stp <input type="checkbox"/> mactable <input type="checkbox"/> rmon
vdsl <input type="checkbox"/> *	<input type="checkbox"/> alarmprofile <input type="checkbox"/> others

The following table describes the labels in this screen.

**Table 163** Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the <b>SNMP Setting</b> screen.  Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See <a href="#">Section 37.3.3 on page 336</a> for individual trap descriptions.  The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 37.3.6 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via Web Configurator at any one time.

- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.



Note: It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure Switch settings.

Click **Management** > **Access Control** > **Logins** to view the screen as shown next.

**Figure 217** Management > Access Control > Logins

The following table describes the labels in this screen.

**Table 164** Management > Access Control > Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the "admin" user name. You cannot change the default administrator user name. Only the administrator has read/write access.
Old Password	Type the existing system password ( <b>1234</b> is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins	You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see the CLI Reference Guide.
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 37.4 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

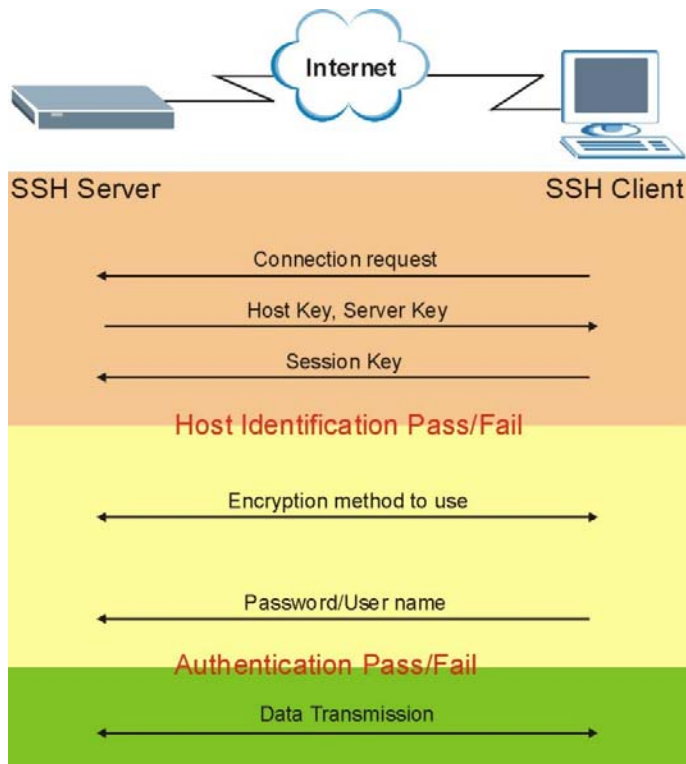
**Figure 218** SSH Communication Example



## 37.5 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

**Figure 219** How SSH Works



### 1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

## 2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

## 3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

# 37.6 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

## 37.6.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

# 37.7 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

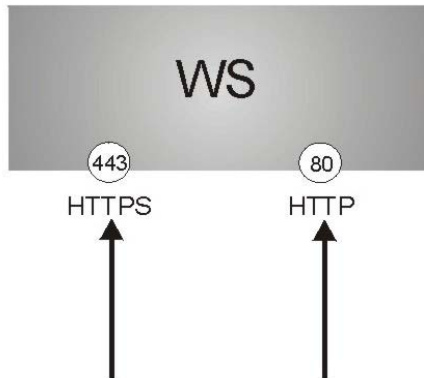
HTTPS on the Switch is used so that you may securely access the Switch using the Web Configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Switch.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).

- 2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

**Figure 220** HTTPS Implementation



Note: If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

## 37.8 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https:// Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

### 37.8.1 Internet Explorer Warning Messages

#### 37.8.1.1 Internet Explorer 6

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

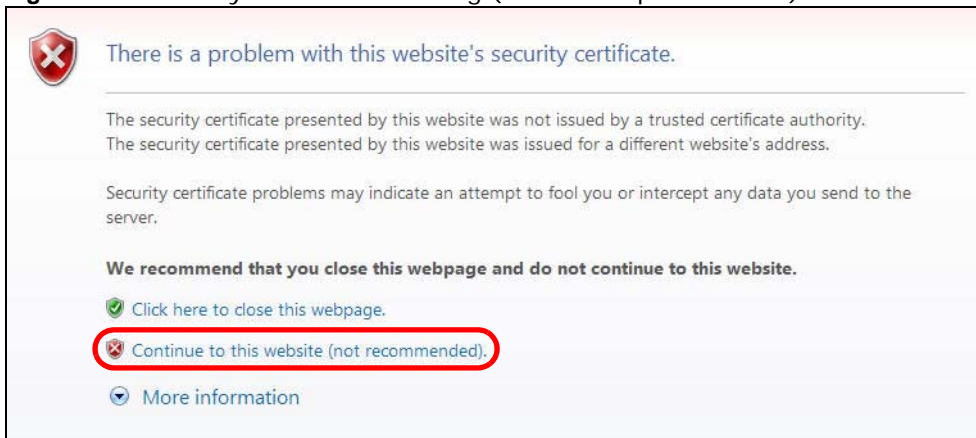
**Figure 221** Security Alert Dialog Box (Internet Explorer 6)



### 37.8.1.2 Internet Explorer 7 or 8

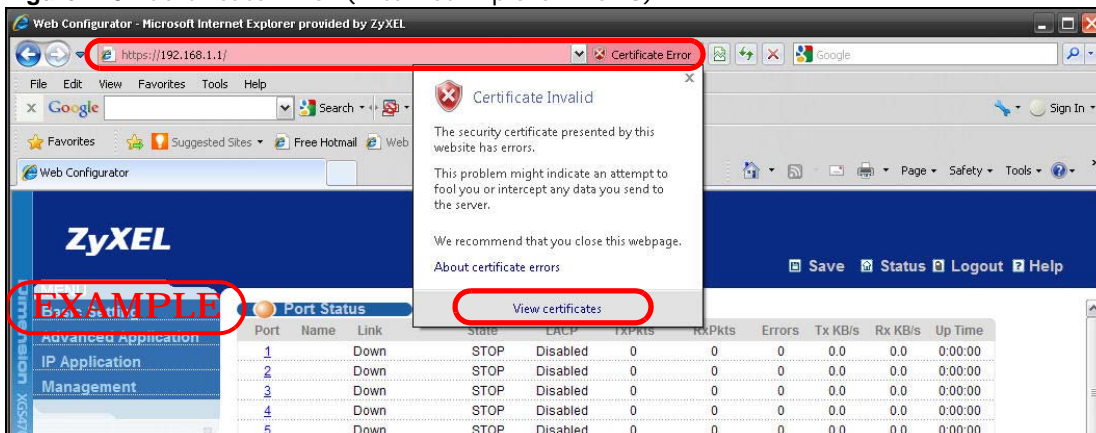
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the web configurator login screen.

**Figure 222** Security Certificate Warning (Internet Explorer 7 or 8)



After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

**Figure 223** Certificate Error (Internet Explorer 7 or 8)



Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

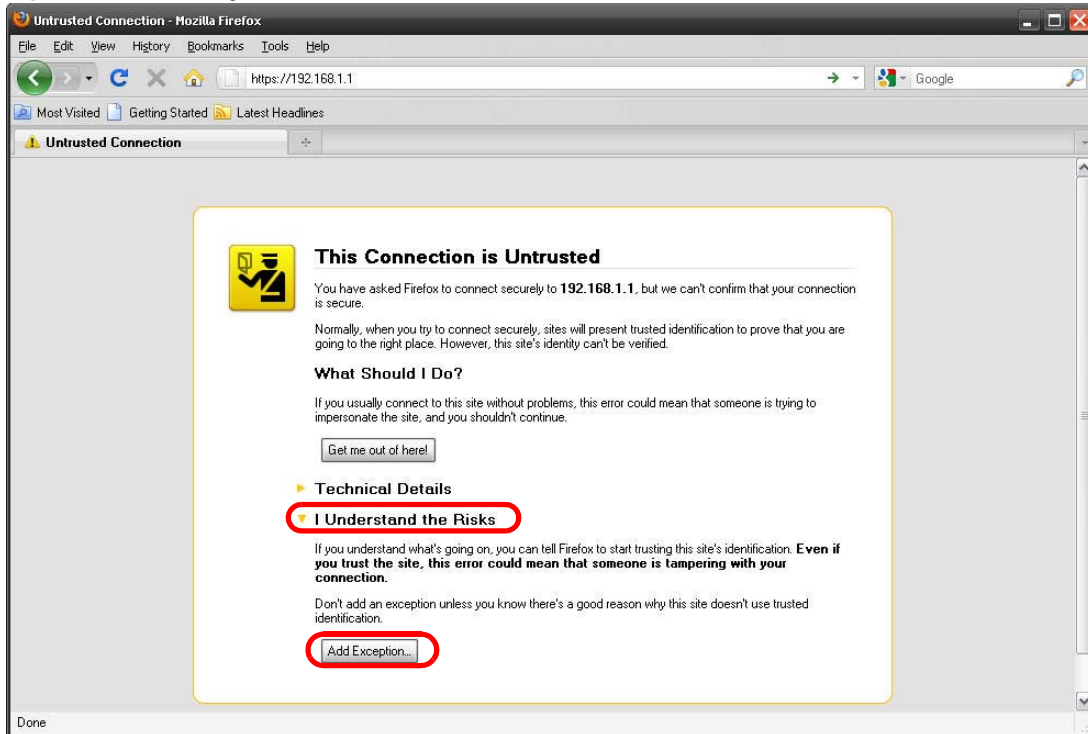
**Figure 224** Certificate (Internet Explorer 7 or 8)



## 37.8.2 Mozilla Firefox Warning Messages

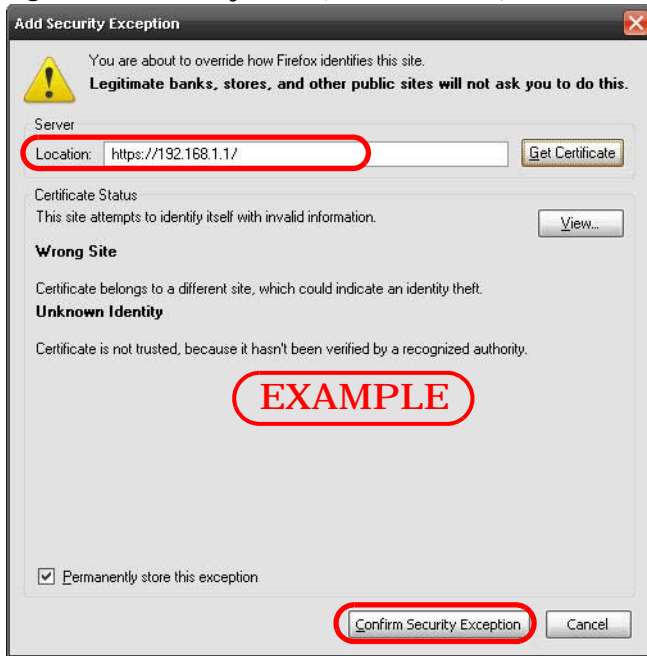
When you attempt to access the Switch HTTPS server, a **This Connection is Untrusted** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

**Figure 225** Security Alert (Mozilla Firefox)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

**Figure 226** Security Alert (Mozilla Firefox)



### 37.8.3 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar (in Internet Explorer 6 or



Mozilla Firefox) or next to the address bar (in Internet Explorer 7 or 8) denotes a secure connection.

**Figure 227** Example: Lock Denoting a Secure Connection

The screenshot shows the ZyXEL Web Configurator interface in Mozilla Firefox. The address bar displays a secure connection: `https://192.168.0.1/`. A red circle highlights the lock icon in the bottom right corner of the browser window. The main content area shows a 'Port Status' table with the following data:

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12	100MF	FORWARDING	FORWARDING	Disabled	84724	285753	0	0.0	0.442	6:03:46
13		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
15		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16		Down	STOP	Disabled	289322	88392	0	0.0	0.0	0:00:00
17		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
18		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

Below the table, there are radio buttons for 'Any' (selected) and 'Port' (with an empty input field), and a 'Clear Counter' button. A red circle highlights the lock icon in the bottom right corner of the browser window.

## 37.9 Service Port Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure "trusted computer(s)" for each service in

the **Remote Management** screen (discussed later). Click **Management > Access Control > Service Access Control** to view the screen as shown.

**Figure 228** Management > Access Control > Service Access Control

Services	Active	Service Port	Timeout
Telnet	<input checked="" type="checkbox"/>	23	
SSH	<input checked="" type="checkbox"/>	22	
FTP	<input checked="" type="checkbox"/>	21	
HTTP	<input checked="" type="checkbox"/>	80	3 Minutes
HTTPS	<input checked="" type="checkbox"/>	443	
ICMP	<input checked="" type="checkbox"/>		
SNMP	<input checked="" type="checkbox"/>		

The following table describes the fields in this screen.

**Table 165** Management > Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the <b>Server Port</b> field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the Web Configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 37.10 Remote Management

Click **Management > Access Control > Remote Management** to view the screen as shown next.

You can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

**Figure 229** Management > Access Control > Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	<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"/>
2	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 166** Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IPv4 or IPv6 address range of trusted computers from which you can manage this Switch.  The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click <b>Apply</b> to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## Diagnostic

This chapter explains the **Diagnostic** screen.

### 38.1 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

**Figure 230** Management > Diagnostic

The screenshot shows the 'Diagnostic' screen with a title bar and a large empty text area labeled '- Info -'. Below this are three main sections: 'System Log' with 'Display' and 'Clear' buttons; 'IP Ping' with radio buttons for 'IPv4' and 'IPv6', dropdown menus for 'Outgoing Interface' (both set to 'default-management'), and empty text boxes for 'VLAN ID'; and 'IP Address' with an empty text box and a 'Ping' button. At the bottom is the 'Port Test' section with a 'Port' dropdown set to '1' and 'Internal Test' and 'External Test' buttons.

The following table describes the labels in this screen.

**Table 167** Management > Diagnostic

LABEL	DESCRIPTION
System Log	Click <b>Display</b> to display a log of events in the multi-line text box. Click <b>Clear</b> to empty the text box and reset the syslog entry.
IP Ping	Select to ping an <b>IPv4</b> or <b>IPv6</b> address, and the interface to send IP ping packets ( <b>default-management</b> , <b>inband-vlan</b> , <b>inband-default</b> , <b>out-of-band</b> ). When you select <b>inband-vlan</b> in the <b>Outgoing interface</b> field, you have to also specify a VLAN ID for the ping conditions.

**Table 167** Management > Diagnostic (continued)

LABEL	DESCRIPTION
IP address	Type the IPv4 or IPv6 address of a device and then click <b>Ping</b> to have the Switch ping the IP address.
Port Test	From the <b>Port</b> drop-down list box, select a port number and click <b>Internal Test</b> to perform an internal loopback test or click <b>External Test</b> (on a VDSL port) to perform a loopback test to the a remote CPE device. A successful or fail test result displays then.

This chapter explains the syslog screens.

## 39.1 Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

**Table 168** Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

## 39.2 Syslog Setup

Click **Management** > **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

**Figure 231** Management > Syslog

Logging type	Active	Facility
System	<input checked="" type="checkbox"/>	local use 0
Interface	<input checked="" type="checkbox"/>	local use 0
Switch	<input checked="" type="checkbox"/>	local use 0
AAA	<input checked="" type="checkbox"/>	local use 0
IP	<input checked="" type="checkbox"/>	local use 0

The following table describes the labels in this screen.

**Table 169** Management > Syslog

LABEL	DESCRIPTION
Syslog	Select <b>Active</b> to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click <b>Apply</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 39.3 Syslog Server Setup

Click **Management > Syslog > Syslog Server Setup** to view the screen as shown next. Use this screen to configure a list of external syslog servers.

**Figure 232** Management > Syslog > Syslog Server Setup

The following table describes the labels in this screen.

**Table 170** Management > Syslog > Syslog Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IPv4 or IPv6 address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click <b>Add</b> to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the <b>Save</b> link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Clear	Click <b>Clear</b> to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays <b>Yes</b> if the device is to send logs to the syslog server. <b>No</b> displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's <b>Delete</b> check box and click <b>Delete</b> to remove the entry.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



## Loop Diagnostic

This chapter explains the **Loop Diagnostic** screen.

### 40.1 Dual-End Loop Test

Click **Management** and **Loop Diagnostic** in the navigation panel to open this screen. Use this screen to perform dual-end loop test for a port. Refer to [Section 7.2.1 on page 54](#) for the port status relationship.

**Figure 233** Loop Diagnostic



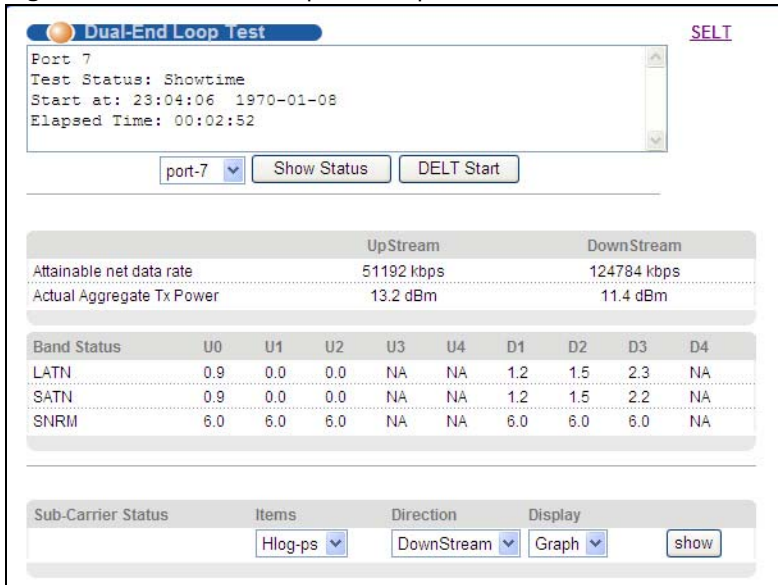
The following table describes the labels in this screen.

**Table 171** Loop Diagnostic

LABEL	DESCRIPTION
Dual-End Loop Test	This field displays a port's current status. The status changes to <b>LD_Testing</b> when you perform a DELT test and it also displays the time you started the test task and how long the test has been proceeded.
Show Status	Select a port number from the drop-down list box and click <b>Show Status</b> to display the test result in the table below.
DELT Start	This button appears when a port's status is "Showtime". Click <b>DELT Start</b> to start the dual-end loop test between the Switch and the remote devices.  Note: It takes several minutes to complete whole test. Before it's completed, the status stays at "LD_Testing".

After the DELT test completes, a summary report displays at the bottom of this screen. This is an example.

**Figure 234** Dual-End Loop Test Report



The following table describes the test report labels in this screen.

**Table 172** Dual-End Loop Test Report

LABEL	DESCRIPTION
Attainable net data rate	The is the maximum upstream/downstream data rate for this line.
Actual Aggregate Tx Power	This is the total amount of upstream/downstream output power for this line.
Band Status	The fields in this section display the status for upstream bands 0, 1, 2, 3, 4 ( <b>U0, U1, U2, U3, U4</b> ) and downstream bands 1, 2, 3, 4 ( <b>D1, D2, D3, D4</b> ).
LATN	This field displays the line attenuation situation in each band. <b>NA</b> displays when the band is not used.
SATN	This field displays the signal attenuation situation in each band. <b>NA</b> displays when the band is not used.
SNRM	This field displays signal-to-noise ratio margin in each band. <b>NA</b> displays when the band is not used.
Sub-Carrier Status	This section allows you to select the criteria and display you the statistics in a raw data list or in a graph.
Items	Select <b>Hlog-ps</b> (Channel Transfer Function per sub-carrier) to see the line's capability against attenuation. Select <b>QLN-ps</b> (Quiet Line Noise per sub-carrier) to see the line's noise level. Select <b>SNR-ps</b> (Signal-to-Noise-Ratio per sub-carrier) to see the line's signal strength level by calculating the ratio between the received signal power and the received noise power for that sub-carrier. Select <b>Hlin-ps</b> to see the line's capability against attenuation.
Direction	Select <b>Downstream</b> or <b>Upstream</b> for the direction.

**Table 172** Dual-End Loop Test Report (continued)

LABEL	DESCRIPTION
Display	Select <b>Graph</b> or <b>Text</b> to display the VDSL sub-carrier status. The <b>Text</b> is available when you select <b>Downstream</b> or <b>Upstream</b> in the <b>Direction</b> field.
show	Select the criteria above and click <b>show</b> to display statistics in a raw data list or in a graph at the bottom of this screen.

## 40.2 Single-End Loop Test (SELT)

Click the **SELT** link at the top-right corner of the **Dual-End Loop Test** screen to open this screen. Use this screen to check the distance to the subscriber's location where the selected port is connected.

**Figure 235** Single Ended Line Test

Items	value	
Loop Type	PE 0.4mm	
Loop length	0 m( 0.000 kft)	
Reflection	1	2
Delay	1.8	64.3
Error	0.1	25.3
Atn@180kHz	1.3	-42.0
Atn@300kHz	0.5	-44.2
FitError	0.5	4.7
Termination	1.00	1.00

The following table describes the labels in this screen.

**Table 173** Single Ended Line Test

LABEL	DESCRIPTION
Single Ended Line Test	This field displays a port's current SELT and calibration status. The status changes to "In Progress" when you perform a SELT or calibration. It also displays the time you started the test task and how long the test has been processed.
Show Status	Select a port number from the drop-down list box and click <b>Show Status</b> to display the test result in the table below.

**Table 173** Single Ended Line Test (continued)

LABEL	DESCRIPTION
SELT Start	<p>Click <b>SELT Start</b> to start a single-end loop test.</p> <p>Note: Connect the Telco-50 connector to the <b>VDSL Line</b> port, but the selected DSL port must have an open loop. There cannot be a DSL device, phone, fax machine or other device connected to the subscriber's end of the VDSL line.</p> <p>The SELT takes at least fifteen seconds. To check the status of a SELT or look at the last SELT result of a port, select the port number from the <b>Port</b> drop-down list box and click <b>Show Status</b>. The results tell you what gauge of telephone wire is connected to the port and the approximate length of the line.</p>
Calibrate	<p>Click <b>Calibrate</b> to reset the SELT parameters on the Switch to achieve high SELT accuracy.</p> <p>Note: Make sure you disconnect the Telco-50 connector from the <b>VDSL Line</b> port before you do calibration.</p>
Loop Type	This field displays what gauge of telephone wire is connected to the port.
Loop length	This field displays the distance from the Switch to the subscriber's location.
Reflection	<p>This field displays the index number of each reflection in a test. Only the first 4 reflection results are displayed.</p> <p>When you perform a SELT, the Switch sends a wideband signal and calculates the loop information from the signal echoes (reflections).</p> <p>Note: Only the reflection from the end of a line indicates proper information for your reference.</p>
Delay	This field displays the estimated delays the Switch calculates from each reflection.
Error	This field displays the estimated errors the Switch calculates from each reflection.
Atn@180kHz	This field displays the estimated attenuation the Switch calculates for the band at 180kHz on the line.
Atn@300kHz	This field displays the estimated attenuation the Switch calculates for the band at 300kHz on the line.
FitError	This field displays an indicator of the error in the attenuation fields.
Termination	This field displays the phase jump at the line termination. A value of <b>0</b> indicates a shortcut termination. A value of <b>1</b> indicates an open termination.

## MAC Table

This chapter introduces the **MAC Table** screen.

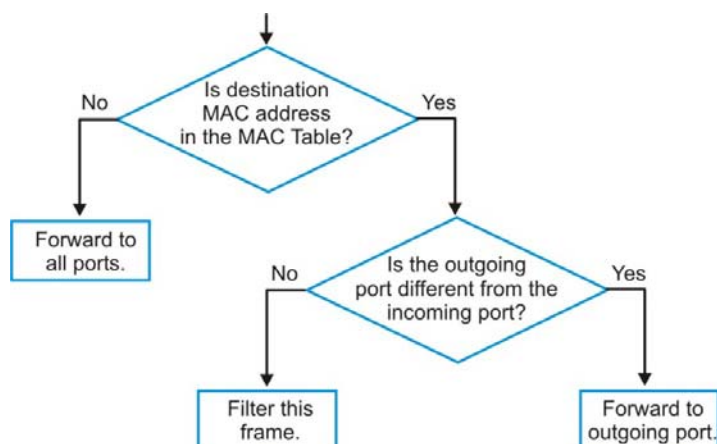
### 41.1 MAC Table Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the MAC table to determine how to forward frames. See the following figure.

- 1 The Switch examines a received frame and learns the port on which this source MAC address came.
- 2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
  - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
  - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
  - If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

**Figure 236** MAC Table Flowchart



## 41.2 Viewing the MAC Table

Click **Management** > **MAC Table** in the navigation panel to display the following screen.

**Figure 237** Management > MAC Table

Index	MAC Address	VID	Port	Type
1	00:02:b3:c9:81:4e	1	25	dynamic
2	00:02:e3:57:ea:1c	1	25	dynamic
3	00:02:e3:57:ea:3d	1	25	dynamic
4	00:04:80:9b:78:00	1	25	dynamic
5	00:0c:29:39:a6:67	1	25	dynamic
6	00:0c:29:49:50:e6	1	25	dynamic

The following table describes the labels in this screen.

**Table 174** Management > MAC Table

LABEL	DESCRIPTION
Mac-flush	Click this link to clear the MAC address table to remove all learned MAC addresses.
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Mac-flush	Select a port or all ports and click this button to clear the MAC address table to remove all learned MAC addresses on the port(s).
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is <b>dynamic</b> (learned by the Switch) or <b>static</b> (manually entered in the <b>Static MAC Forwarding</b> screen).

## ARP Table

This chapter introduces ARP Table.

### 42.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

#### 42.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

### 42.2 Viewing the ARP Table

Click **Management** > **ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s).

**Figure 238** Management > ARP Table



Index	IP Address	MAC Address	VID	Type	Age(s)
1	172.18.31.40	00:21:85:0c:44:4b	1	dynamic	300

The following table describes the labels in this screen.

**Table 175** Management > ARP Table

<b>LABEL</b>	<b>DESCRIPTION</b>
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a Switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
VID	This is the ID number of the VLAN to which the MAC address belongs.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static.
Age(s)	This shows how long (in second) the entry remains valid. Zero means the entry is always valid.



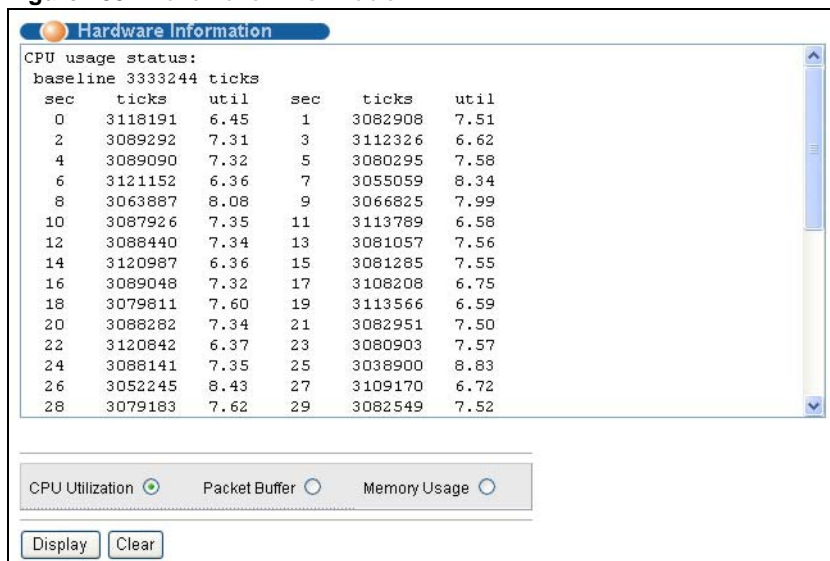
## Hardware Information

This chapter explains the **Hardware Information** screen.

### 43.1 Hardware Information

Click **Management** > **Hardware** in the navigation panel to open this screen. Use this screen to check current detailed hardware information for such as CPU, packet buffer, and memory utilization.

**Figure 239** Hardware Information



The following table describes the labels in this screen.

**Table 176** Hardware Information

LABEL	DESCRIPTION
CPU Utilization	Select this and then click <b>Display</b> to see detailed CPU usage. It contains such as how long the CPU has been running since the Switch is up and how many percentage of the CPU is currently used.
Packet Buffer	Select this and then click <b>Display</b> to see detailed packet buffer usage.
Memory Usage	Select this and then click <b>Display</b> to see detailed memory usage.
Clear	Click this to clear this screen.

## CFM Action

This chapter explains the **CFM (Connectivity Fault Management) Action** screen. Refer to [Section 28.1 on page 274](#) to see more information.

### 44.1 CFM Action

Click **Management** and **CFM Action** in the navigation panel to open this screen. Use this screen to manage any connectivity faults.

**Figure 240** CFM Action

The following table describes the labels in this screen.

**Table 177** CFM Action

LABEL	DESCRIPTION
Continuity Check	Select a level, type a VLAN ID and click <b>Enable</b> or <b>Disable</b> to start or disable sending the connectivity check packets in this MD (Maintenance Domain).
Link Trace	Select this to trace the nodes on this link.
Loop Back	Select this to perform a loopback test on this link.
Level	Select an MD level (0-7).
VID	Type an MA VLAN ID (0-4096) under the MD level.
MEPID	Type an MEP ID to specify which MEP port on the device initiates the action.

**Table 177** CFM Action

LABEL	DESCRIPTION
Destination MAC	Enter the destination port's MAC address which you want to trace the link to. <b>Note:</b> The destination must be an MEP port.
Count	This is how many times you want to perform for the test.
TransID	This is available after you complete a link trace. This is an increasing number to display how many times the test was done for an MEP port. Enter a <b>TransID</b> and an <b>EntryNum</b> you get from a test report, and click <b>Show Result</b> to see detailed information.
EntryNum	This is available after you complete a link trace. This displays how many nodes traced in a test. Enter a <b>TransID</b> and an <b>EntryNum</b> you get from a test report, and click <b>Show Result</b> to see detailed information.
Transmit	Click this to start the connectivity test.
Show Result	Select a level, type a VID and MEPID and click this to display the result for a test.

Examples of connectivity test reports are shown next.

**Figure 241** Connectivity Test Report Examples

The figure displays three screenshots of connectivity test reports from a network management interface, each titled 'Connectivity Fault Management'.

**LoopBack Report:** The report shows the following status:

```

someMACstatusDefect: No
someRMEPCCMdefect: No
errorCCMdefect: No
xcconCCMdefect: No
CCMsequenceErrors: 0
CCIsentCCMs: 100
nextLBMtransID: 5
expectedLBRtransID: 5
inorderLBRs: 5
outorderLBRs: 0
unmatchedLBRs: 0
nextLTMtransID: 0
unexpectedLTRs: 0
transmittedLBRs: 0

```

**Link Trace Report:** The report shows a table with the following data:

TransID	TTL	FDBOnly	Entries	Dest. MAC
0	64	No	1	00:19:cb:14:25:37

**Show Detail Report:** The report shows the following details:

```

ltnreplylist level 2 vlan 101 mepid 1 transid 0
LTR 1:
Replied TTL: 63
Ingress MAC: 00:19:cb:14:25:4f
Egress MAC: 00:19:cb:14:25:37

```

## IPv6 Cache

This chapter describe the IPv6 caches on the Switch. Refer to [Section 8.6 on page 76](#) to see more information about IPv6.

### 45.1 Overview

The Switch uses the Neighbor Discovery Protocol (NDP) to discover other IPv6 devices and track their reachability in a network. The Switch uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Switch maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Switch configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Switch also sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Switch uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Switch creates an entry in the default router list cache if the router can be used as a default router.

When the Switch needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Switch uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is on-link, the address is considered as the next hop. Otherwise, the Switch determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Switch looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

## 45.2 Neighbor Cache

Click **Management** > **IPv6 Cache** in the navigation panel to open this screen. The neighbor cache is similar to a MAC address table in IPv4. Use this screen to view the link-layer addresses of the Switch's interfaces and neighboring devices. You can also see if a neighbor is still reachable from the Switch.

**Figure 242** IPv6 Cache > Neighbor Cache

Index	Neighbor	MAC	State	Link Type	Interface
1	3ffe:501:ffff:100:ce5d:4eff:fe00:2	cc:5d:4e:00:00:02	Reachable	Local	VLAN100
2	fe80::1111	11:22:33:44:55:66	Reachable	Static	VLAN1
3	fe80::200:ff:fe00:a0a0	00:00:00:00:00:00	Invalid	Dynamic	VLAN1
4	fe80::ce5d:4eff:fe00:2	cc:5d:4e:00:00:02	Reachable	Local	VLAN1
5	fe80::ce5d:4eff:fe00:1	cc:5d:4e:00:00:01	Reachable	Local	MGMT0
6	fe80::ce5d:4eff:fe00:2	cc:5d:4e:00:00:02	Reachable	Local	VLAN100

The following table describes the labels in this screen.

**Table 178** IPv6 Cache > Neighbor Cache

LABEL	DESCRIPTION
reload	Select <b>ALL</b> or a specific interface and then click the <b>reload</b> button to display information about all or related IPv6 neighboring interfaces on this screen.
Index	This is the index number of the entry.
Neighbor	This is the IPv6 address of a neighbor or the Switch's interface.
MAC	This is the MAC address of the interface on which the IPv6 address is configured.
State	<p>This field displays whether the neighboring IPv6 interface is reachable. In IPv6, "reachable" means an IPv6 packet can be correctly forwarded to a neighboring node (host or router) and the neighbor can successfully receive and handle the packet. The options that can display in this field are:</p> <p><b>Reachable:</b> The interface of the neighboring device is reachable. (The Switch has received a response to its neighbor solicitation.)</p> <p><b>Stale:</b> The last reachable time has expired or the Switch received an unrequested advertisement that updates the cached link-layer address from the neighboring interface.</p> <p><b>Delay:</b> A packet is being sent to the neighboring interface in <b>Stale</b> state. The Switch delays sending request packets for a short time to give upper-layer protocols a chance to determine reachability. If no reachability confirmation is received within the delay time period, the Switch sends a neighbor solicitation and changes the state to <b>Probe</b>.</p> <p><b>Probe:</b> The Switch is sending neighbor solicitations and waiting for the neighbor's response.</p> <p><b>Invalid:</b> The neighbor address is an invalid IPv6 address.</p> <p><b>Unknown:</b> The status of the neighboring interface cannot be determined.</p> <p><b>Incomplete:</b> Address resolution is in progress and the link-layer address of the neighbor has not yet been determined (see RFC 4861). The interface of the neighboring device did not give a complete response.</p>

**Table 178** IPv6 Cache > Neighbor Cache (continued)

LABEL	DESCRIPTION
Link Type	This field displays the type of the IPv6 address.  <b>Local:</b> The IPv6 address belongs to an interface on the Switch.  <b>Static:</b> The IPv6 address belongs to a neighboring interface and it has been configured manually on the Switch.  <b>Dynamic:</b> The IPv6 address belongs to a neighboring interface and the Switch has learned it dynamically.  <b>Other:</b> The IPv6 address belongs to none of the types above.
Interface	If the link type is <b>Local</b> , this field displays the name of the interface. If the link type is any of the others, this field displays the name of an interface on the Switch, through which the Switch can reach the neighboring interface.

## 45.3 Router

Click **Management** > **IPv6 Cache** in the navigation panel and then the **Router** link to open this screen. Use this screen to view the IPv6 router advertisement information on the Switch.

**Figure 243** IPv6 Cache > Router

The screenshot shows a web interface for 'Router Info' with tabs for 'Neighbor' and 'Path MTU'. A dropdown menu is set to 'VLAN1'. Below the title 'Show Router Advertisement Information' is a table with the following data:

Interface Name	Item	Status
VLAN1	Router	fe80::200:ff:fe00:a0a0
	Hop Limit	64
	Lifetime(sec)	1800
	M-flag	0
	O-flag	0
	Reachable Time(ms)	30000
	Retransmit Time(ms)	1000
	MTU	
	Prefix	3ffe:501:fff:100::/64
	On-link	1
	Autoconfig	1
	Valid lifetime(sec)	2592000
	Preferred lifetime(sec)	604800

The following table describes the labels in this screen.

**Table 179** IPv6 Cache > Router

LABEL	DESCRIPTION
	Select an interface from the drop-down list box to view the router advertisement information the interface has received.
Interface Name	This field displays the name of the interface.
Item	This field displays the name of an item carried by router advertisements.
Status	This field displays the item's status details.

**Table 179** IPv6 Cache > Router

LABEL	DESCRIPTION
Router	This field displays the router's IPv6 address for the route through this interface.
Hop Limit	When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.  This field displays the maximum number of network segments that a packet can cross before reaching the destination. <b>0</b> displays if the router does not specify the setting.
Lifetime(sec)	This is the number of seconds in which hosts can use the router as the default router. 0 displays if the router is not a default router.
M-flag	This field displays <b>1</b> if the Switch indicates to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Otherwise, <b>0</b> displays if the Switch indicates to hosts that DHCPv6 is not available and they should use the prefix in router advertisements the router sends.
O-flag	This field displays <b>1</b> if the Switch indicates to hosts to obtain DNS information through DHCPv6. Otherwise, 0 displays if the Switch indicates to hosts that DNS information is not available in this network.
Reachable Time(ms)	This is the time in milliseconds the router can wait for a neighbor device's reachability confirmation before the router determines the device is not reachable. <b>0</b> displays if the router does not specify the setting.
Retransmit Time(ms)	The is the time in milliseconds the router waits before resending a neighbor solicitation packet. 0 displays if the router does not specify the setting.
MTU	The Maximum Transmission Unit. This field displays the maximum size of each IPv6 data packet, in bytes, that this router can accept. If a larger packet arrives, the Switch divides it into smaller fragments before forwarding them to the router.
Prefix	This field displays the network address used for host stateless address autoconfiguration.
On-link	This field displays <b>1</b> if the Switch can use this prefix for on-link determination. Otherwise, it displays <b>0</b> .  A prefix is considered to be on-link when it is assigned to an interface on a link. It's used to determine if an address is on the Switch's subnet and can be reached directly without passing through a router. An on-link interface is directly connected to the Switch or connected through another switch.  If the Switch sends a packet to a host and the destination IP address is off-link, the packet will be sent to a next-hop (a router in the router list) for this destination. If the destination host is on-link, it is also the next hop.
Autoconfig	This field displays <b>1</b> if hosts can use this prefix for stateless address autoconfiguration. Otherwise, it displays <b>0</b> .
Valid lifetime(sec)	This field displays how long in seconds the prefix is valid for on-link determination.
Preferred lifetime(sec)	This field displays how long in seconds addresses generated from the prefix via stateless address autoconfiguration remain preferred.

## 45.4 Path MTU

Click the **Path MTU** link in the **Management > IPv6 Cache** screen to open the following screen. Use this screen to check IPv6 path MTU sizes. In IPv6, packets can be fragmented only by the source device from which the packets are sent. The source device must adjust the MTU size if it

receives a “Packet Too Big” notification from its router. This screen’s path MTU table lists different MTU sizes and expiration information for data transmissions with different routers.

**Figure 244** IPv6 Cache > Path MTU



The following table describes the labels in this screen.

**Table 180** IPv6 Cache > Path MTU

LABEL	DESCRIPTION
Path MTU aging time	This field shows how long entries remain in this path MTU table before they age out.
Index	This is the index number of an entry.
Destination Address	This is the IPv6 address of a destination host.
MTU	This is the maximum transmission unit used for data transmission to the destination host.
Expire	This is the remaining time before the entry expires.



# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [Switch Access and Login](#)
- [Switch Configuration](#)

## 46.1 Power, Hardware Connections, and LEDs

---

The Switch does not turn on. None of the LEDs turn on.

---

- 1 Make sure the Switch is turned on (in DC models or if the DC power supply is connected in AC/DC models).
- 2 Make sure you are using the power adaptor or cord included with the Switch.
- 3 Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
- 5 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
- 6 If the problem continues, contact the vendor.

---

The **ALM** LED is on.

---

- 1 Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
- 2 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
- 3 If the problem continues, contact the vendor.

---

One of the LEDs does not behave as expected.

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 3.2 on page 31](#).
- 2 Check the hardware connections. See [Section 46.1 on page 377](#).
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
- 5 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
- 6 If the problem continues, contact the vendor.

## 46.2 Switch Access and Login

---

I forgot the IP address for the Switch.

---

- 1 The default in-band management IP address is **192.168.1.1**.
- 2 Use the console port to log in to the Switch.
- 3 Use the **MGMT** port to log in to the Switch, the default management IP address of the **MGMT** port is 192.168.0.1.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 4.6 on page 40](#).

---

I forgot the username and/or password.

---

- 1 The default username is **admin** and the default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 4.6 on page 40](#).

---

I cannot see or access the **Login** screen in the Web Configurator.

---

- 1 Make sure you are using the correct IP address.

- The default in-band IPv4 address is [192.168.1.1](#) and out-of-band IPv4 address is [192.168.0.1](#).
  - If you changed the IP address, use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Switch](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 3.2 on page 31](#).
  - 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
  - 4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)
  - 5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See [Section 4.6 on page 40](#).
  - 6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

---

#### I can see the **Login** screen, but I cannot log in to the Switch.

---

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.  
  
Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
- 3 Disconnect and re-connect the cord to the Switch.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 4.6 on page 40](#).

---

#### Pop-up Windows, JavaScripts and Java Permissions

---

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).

- Java permissions (enabled by default).

---

I cannot see some of **Advanced Application** submenus at the bottom of the navigation panel.

---

The recommended screen resolution is 1024 by 768 pixels. Adjust the value in your computer and then you should see the rest of **Advanced Application** submenus at the bottom of the navigation panel.

---

There is unauthorized access to my Switch via telnet, HTTP and SSH.

---

Click the **Display** button in the **System Log** field in the **Management > Diagnostic** screen to check for unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **Management > Access Control > Remote Management** screen for telnet, HTTP and SSH (see [Section 37.10 on page 354](#)). Computers not belonging to the secured client set cannot get permission to access the Switch.

## 46.3 Switch Configuration

---

I lost my configuration settings after I restarted the Switch.

---

Make sure you save your configuration into the Switch's nonvolatile memory each time you make changes. Click **Save** at the top right corner of the Web Configurator to save the configuration permanently. See also [Section 36.6 on page 331](#) for more information about how to save your configuration.



## Product Specifications

The following tables summarize the Switch's hardware and firmware features.

**Table 181** Hardware Specifications

SPECIFICATION	DESCRIPTION
Default IPv4 Address	In-band: 192.168.1.1 Out-of-band (Management port): 192.168.0.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
General Product Specifications	
VDSL	Duplex Method: DMT/FDD Band Plan: 998
Interfaces	Two Gigabit/mini-GBIC uplink ports One Console port One Alarm port Two Telco-50 connectors (for 24 VDSL/POTS lines)
Compatible CPE Device Model	At the time of writing, ZyXEL P-870H-51, P-870HA, P-870HW-51, P873 and P874 are the compatible CPE device models.
Performance and Management Specifications	
VDSL	Fixed Rate, Rate Adaptive and dynamic mode. Upstream and Downstream Power back off (UPBO, DPBO) Interleave delay setting RFI configuration Resynchronization

**Table 181** Hardware Specifications

Diagnostics Capabilities	<p>The switch can perform self-diagnostic tests. These tests check the operation of the following circuits:</p> <ul style="list-style-type: none"> <li>FLASH memory</li> <li>DRAM</li> <li>LAN port local and remote loopback test</li> <li>Per VDSL port loopback test</li> <li>HTP items</li> </ul> <p>The switch can also perform dual-end loop diagnostic tests and generate reports with the following formats in a raw data list or in a graph.</p> <ul style="list-style-type: none"> <li>Hlog</li> <li>QLN</li> <li>SNR</li> </ul>
Bridging	<ul style="list-style-type: none"> <li>16K MAC addresses</li> <li>Static MAC address filtering by source/destination</li> <li>Broadcast storm control</li> <li>Static MAC address forwarding</li> </ul>
Switching	<ul style="list-style-type: none"> <li>Switching fabric: 12.8 Gbps, non-blocking</li> <li>Max. Frame size: 9 K bytes</li> <li>Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE</li> <li>Prevent the forwarding of corrupted packets</li> </ul>
STP	<ul style="list-style-type: none"> <li>IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)</li> <li>Multiple Rapid Spanning Tree capability (2 configurable trees)</li> <li>IEEE 802.1s Multiple Spanning Tree Protocol</li> </ul>
QoS	<ul style="list-style-type: none"> <li>IEEE 802.1p</li> <li>SPO, WRR, WFQ, SPO/WRR or SPO/WFQ combination capable</li> <li>Eight priority queues per port</li> <li>Rule-based bandwidth control (ingress traffic metering/dropping 64Kb stepping)</li> <li>Port-based egress traffic shaping</li> <li>Rule-based traffic mirroring</li> <li>IGMP snooping</li> <li>TRTCM</li> </ul>

**Table 181** Hardware Specifications

VLAN	Port-based VLAN 802.1Q tag-based VLAN number of VLAN: 4K, 2000 static maximum GVRP for dynamic registration Double tagging for VLAN stacking Private VLAN for port isolation. Protocol-based VLAN. IP subnet-based VLAN MAC-based VLAN
Port Aggregation	IEEE 802.3ad LACP One group for two Gigabit Ethernet ports
Port mirroring	Rule-based port mirroring Port-based mirroring Support port mirroring per IP/TCP/UDP
Bandwidth control	Supports rate limiting at 64 Kb increments TRTCM
IP Capability	IPv4 and IPv6 support 64 Management IPv4 addresses Wire speed IP forwarding
Routing protocols	Static Routing
IP services	DHCP client DHCP relay VLAN-based DHCP relay
Filtering	Support L2 MAC filtering, L3 IP filtering, Layer 4 TCP/UDP socket
Multicast	IGMP snooping (IGMP v1/v2/v3, 16 VLAN maximum-user configurable) MLD v1/v2 IGMP filtering MVR IGMP timer Multicast reserve group

**Table 181** Hardware Specifications

Security	Static MAC address filtering Static MAC address forwarding MAC Freeze IEEE 802.1x port-based authentication Limiting number of dynamic MAC addresses per port SSH v1/v2 SSL Multiple RADIUS servers Multiple TACACS+ servers 802.1X VLAN and bandwidth assignment. MAC authentication
Physical and Environmental Specifications	
Dimensions	Standard 19" rack mountable 440 mm (W) x 250 mm (L) x 44.35 mm (H) Height: 1U
Weight	5.3 kg
Power Specification	AC (dual input ranges): 100 VAC to 120 VAC, 50/60 Hz $\pm$ 3 Hz, 1.4 A Max. 220 VAC to 240 VAC, 50/60 Hz $\pm$ 3 Hz, 1 A Max. DC input: -36 VDC to -72 VDC, 2 A Max. Note: There is no tolerance for the DC input voltage.
Power Consumption	Support COC version 4
LEDs	Per switch: PWR, SYS, ALM Per Fast Ethernet RJ-45 port: 10 M, 100 M, 1000 M Per mini-GBIC slot: LNK, ACT Per Management port: 10 M, 100 M
Operating Environment	Temperature: -40° C ~ 65° C (-40° F ~ 149° F) Humidity: 10 ~ 95% (non-condensing)
Storage Environment	Temperature: -40° C ~ 70° C (-40° F ~ 158° F) Humidity: 5 ~ 95% (non-condensing)
Ground Wire Gauge	18 AWG or larger
Power Wire Gauge	18 AWG or larger

**Table 182** Firmware Specifications

FEATURE	DESCRIPTION
Number of Login Accounts Configurable on the Switch	4 management accounts configured on the Switch. Authentication via RADIUS and TACACS+ also available.
Maximum Frame Size	9 K (9216 bytes)



**Table 182** Firmware Specifications

FEATURE	DESCRIPTION
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
VLAN Stacking	Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
DHCP (Dynamic Host Configuration Protocol) Relay	Use this feature to have the Switch forward DHCP requests to DHCP servers on your network.
IGMP Snooping	The Switch supports IGMP snooping, enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your Switch.
Differentiated Services (DiffServ)	With DiffServ, the switch marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Two Rate Three Color Marker	Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Classifier and Policy	You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc.
Queuing	Queuing is used to help solve performance degradation when there is network congestion. The following scheduling services are supported: Strict Priority Queuing (SPQ) Weighted Round Robin (WRR), and Weighted Fair Queuing (WFQ). This allows the Switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.
Bandwidth Control	Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.
Broadcast Storm Control	Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes allow the Switch to communicate with management stations not reachable via the default gateway.
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network.  This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

**Table 182** Firmware Specifications

FEATURE	DESCRIPTION
IP Multicast	With IP multicast, the Switch delivers IP packets to a group of hosts on the network-not everybody. In addition, the Switch can send packets to Ethernet devices that are not VLAN-aware by untagging (removing the VLAN tags) IP multicast packets.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)/MSTP (Multiple Spanning Tree Protocol)	(M)(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (M)(R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.
Loop Guard	Use the loop guard feature to protect against network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized DHCP and ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.
Authentication and Accounting	The Switch supports authentication and accounting services via RADIUS and TACACS+ Authentication servers.
Device Management	Use the Web Configurator or commands to easily configure the rich range of features on the Switch.
Port Cloning	Use the port cloning feature to copy the settings you configure on one port to another port or ports.
Syslog	The Switch can generate syslog messages and send it to a syslog server.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator, CLI or an FTP/TFTP tool to put it on the Switch.  <b>Note: Only upload firmware for your specific model!</b>
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.
VDSL Template	At the time of writing, you can configure one VDSL line profile and VDSL channel profile in one VDSL template on the Switch.

The following list, which is not exhaustive, illustrates the standards supported in the Switch.

**Table 183** Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 894	Ethernet II Encapsulation
RFC 1112	IGMP v1
RFC 1155	SMI
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II

**Table 183** Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2698	Two Rate Three Color Marker (trTCM)
RFC 2865	RADIUS - Vendor Specific Attribute
RFC 2674	P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 3046	DHCP Relay
RFC 3164	Syslog
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3)
RFC 3580	RADIUS - Tunnel Protocol Attribute
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1D	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1Q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation
IEEE 802.3ah	Ethernet OAM (Operations, Administration and Maintenance)
IEEE 802.3x	Flow Control
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

## Splitter Board Specifications

The following table lists the splitter board specifications.

**Table 184** CO Impedance Splitter Board Specifications

COUNTRY	POTS
Taiwan	900Ω

## Hardware Telco-50 Connector Pin Assignments

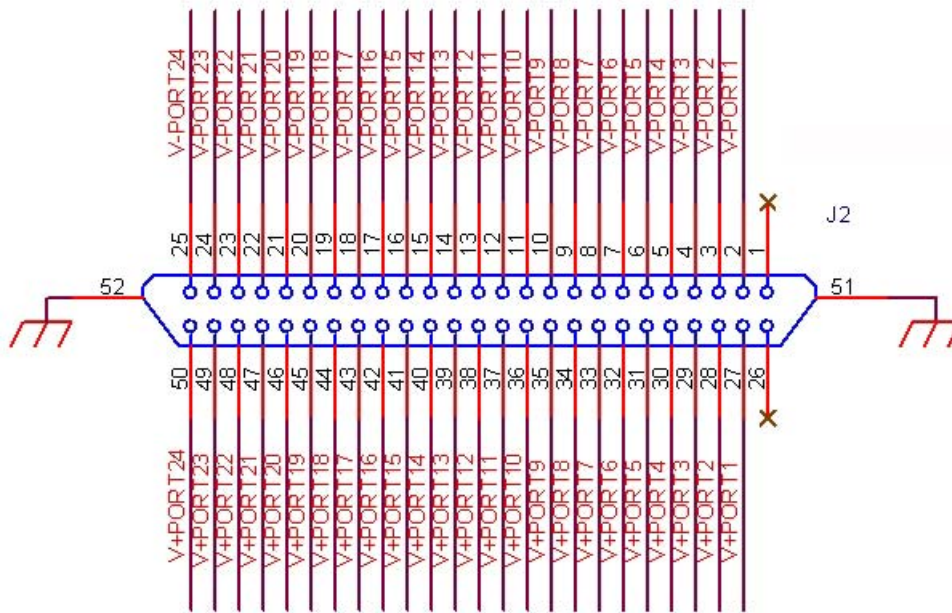
Use Telco-50 cables to connect the **VDSL LINE** port to the user equipment (VDSL modem) and the **POTS LINE** port to the central office switch or PBX (Private Branch Exchange). In this switch, both

VDSL and POTS use same pin assignments. The following table and diagram show the pin assignments of the Telco-50 connectors on the Switch.

**Table 185** Hardware Telco-50 Pin Assignments (VES1724-56)

VDSL				POTS			
PIN1	NULL	PIN26	NULL	PIN1	NULL	PIN26	NULL
PIN2	V-PORT1	PIN27	V+PORT1	PIN2	V-PORT1	PIN27	V+PORT1
PIN3	V-PORT2	PIN28	V+PORT2	PIN3	V-PORT2	PIN28	V+PORT2
PIN4	V-PORT3	PIN29	V+PORT3	PIN4	V-PORT3	PIN29	V+PORT3
PIN5	V-PORT4	PIN30	V+PORT4	PIN5	V-PORT4	PIN30	V+PORT4
PIN6	V-PORT5	PIN31	V+PORT5	PIN6	V-PORT5	PIN31	V+PORT5
PIN7	V-PORT6	PIN32	V+PORT6	PIN7	V-PORT6	PIN32	V+PORT6
PIN8	V-PORT7	PIN33	V+PORT7	PIN8	V-PORT7	PIN33	V+PORT7
PIN9	V-PORT8	PIN34	V+PORT8	PIN9	V-PORT8	PIN34	V+PORT8
PIN10	V-PORT9	PIN35	V+PORT9	PIN10	V-PORT9	PIN35	V+PORT9
PIN11	V-PORT10	PIN36	V+PORT10	PIN11	V-PORT10	PIN36	V+PORT10
PIN12	V-PORT11	PIN37	V+PORT11	PIN12	V-PORT11	PIN37	V+PORT11
PIN13	V-PORT12	PIN38	V+PORT12	PIN13	V-PORT12	PIN38	V+PORT12
PIN14	V-PORT13	PIN39	V+PORT13	PIN14	V-PORT13	PIN39	V+PORT13
PIN15	V-PORT14	PIN40	V+PORT14	PIN15	V-PORT14	PIN40	V+PORT14
PIN16	V-PORT15	PIN41	V+PORT15	PIN16	V-PORT15	PIN41	V+PORT15
PIN17	V-PORT16	PIN42	V+PORT16	PIN17	V-PORT16	PIN42	V+PORT16
PIN18	V-PORT17	PIN43	V+PORT17	PIN18	V-PORT17	PIN43	V+PORT17
PIN19	V-PORT18	PIN44	V+PORT18	PIN19	V-PORT18	PIN44	V+PORT18
PIN20	V-PORT19	PIN45	V+PORT19	PIN20	V-PORT19	PIN45	V+PORT19
PIN21	V-PORT20	PIN46	V+PORT20	PIN21	V-PORT20	PIN46	V+PORT20
PIN22	V-PORT21	PIN47	V+PORT21	PIN22	V-PORT21	PIN47	V+PORT21
PIN23	V-PORT22	PIN48	V+PORT22	PIN23	V-PORT22	PIN48	V+PORT22
PIN24	V-PORT23	PIN49	V+PORT23	PIN24	V-PORT23	PIN49	V+PORT23
PIN25	V-PORT24	PIN50	V+PORT24	PIN25	V-PORT24	PIN50	V+PORT24

**Figure 245** Hardware Telco-50 Female Pin Assignments



This table lists the ports and matching pin numbers for the hardware Telco-50 connector.

**Table 186** Hardware Telco-50 Connector Port and Pin Numbers

VDSL PORT NUMBER	PIN NUMBER
1	2, 27
2	3, 28
3	4, 29
4	5, 30
5	6, 31
6	7, 32
7	8, 33
8	9, 34
9	10, 35
10	11, 36
11	12, 37
12	13, 38
13	14, 39
14	15, 40
15	16, 41
16	17, 42
17	18, 43
18	19, 44
19	20, 45
20	21, 46
21	22, 47
22	23, 48

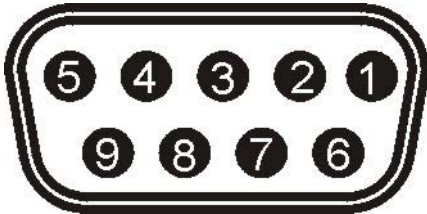
**Table 186** Hardware Telco-50 Connector Port and Pin Numbers (continued)

VDSL PORT NUMBER	PIN NUMBER
23	24, 49
24	25, 50

## Console Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The Switch is DCE when you connect a computer to the console port. The following diagrams and chart show the pin assignments of the console cable.

The pin layout for the DB-9 connector end of the cables is as follows.

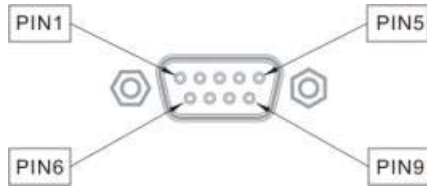
**Figure 246** Console Cable DB-9 Female Pin Layout**Table 187** Console Port Female Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F
Pin 1 = NON
Pin 2 = DCE-TXD
Pin 3 = DCE –RXD
Pin 4 = DCE –DSR
Pin 5 = GND
Pin 6 = DCE –DTR
Pin 7 = DCE –CTS
Pin 8 = DCE –RTS
PIN 9 = NON

## Alarm Port Pin Assignments

The ALARM port is a male 9-pin connector. The following figure shows the pin assignments.

**Figure 247** Alarm Port: Pin Assignment



The following table describes the alarm pins.









**Table 188** Alarm Port: Pin Assignment

ALARM INPUT	PIN	DESCRIPTION
1	Pin 2 and Pin 6	An open circuit for pins 2 and 6 indicates no alarm status. A closed circuit indicates an alarm status.
2	Pin 3 and Pin 7	An open circuit for pins 3 and 7 indicates no alarm status. A closed circuit indicates an alarm status.
3	Pin 4 and Pin 8	An open circuit for pins 4 and 8 indicates no alarm status. A closed circuit indicates an alarm status.
4	Pin 5 and Pin 9	An open circuit for pins 5 and 9 indicates no alarm status. A closed circuit indicates an alarm status.

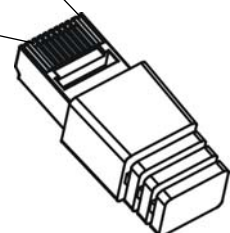


## Ethernet Cable Specifications

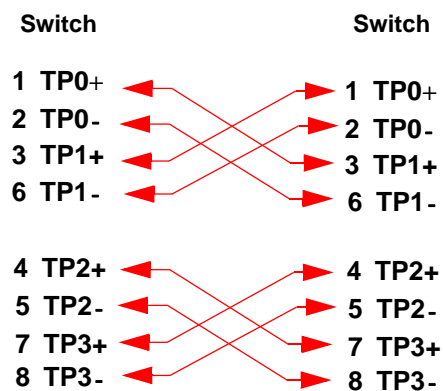
**Table 189** Ethernet Cable Pin Assignments

WAN / LAN ETHERNET CABLE PIN LAYOUT							
Straight-through				Crossover			
(Switch)		(Adapter)		(Switch)		(Switch)	
1	IRD +		1	OTD +		1	IRD +
2	IRD -		2	OTD -		2	IRD -
3	OTD +		3	IRD +		3	OTD +
6	OTD -		6	IRD -		6	OTD -

**Table 190** 1000BASE-T (Straight-through) Cat5e Ethernet Cable

PIN	PAIR	WIRE	COLOR	PINS ON PLUG
1	2	1	White/Orange	
2	2	2	Orange	
3	3	1	White/Green	
4	1	2	Blue	
5	1	1	White/Blue	
6	3	2	Green	
7	4	1	White/Brown	
8	4	2	Brown	

**Figure 248** Twisted-Pair 1000BASE-T Ethernet Cable Schematic



## Telco-50 Pin Color

**Table 191** Telco-50 Pin Color

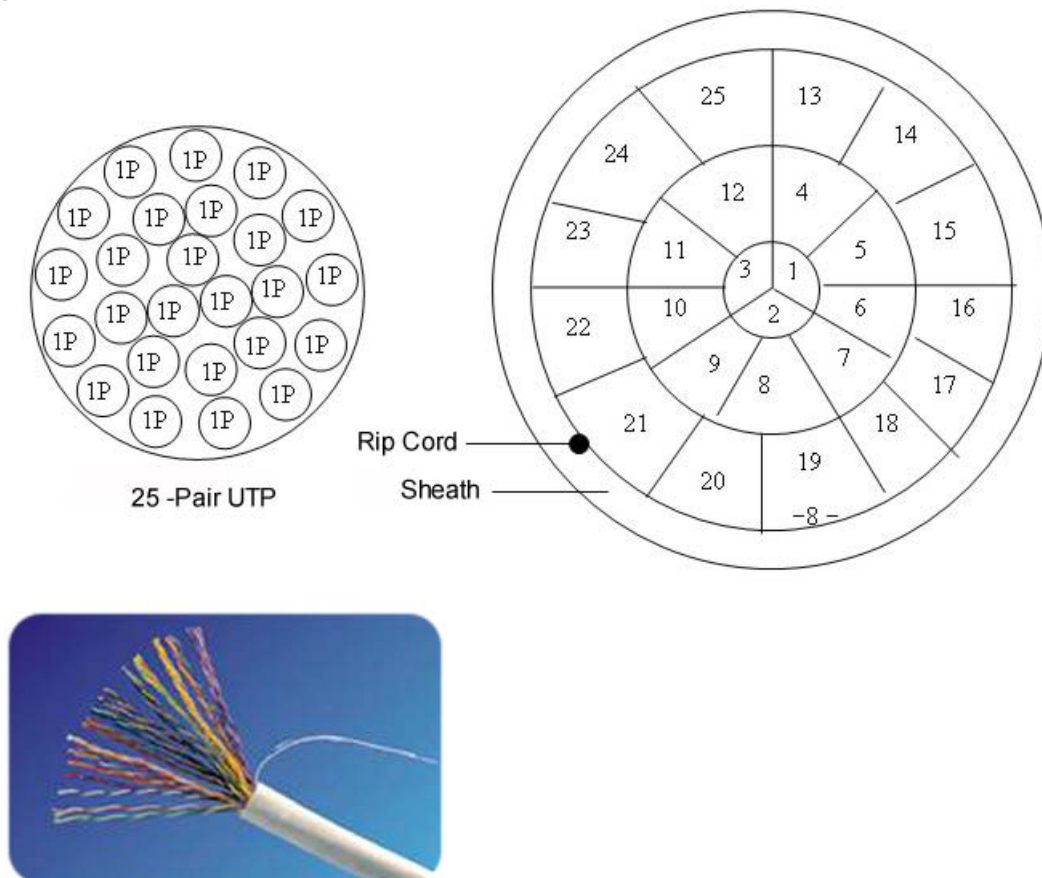
LOGARITHM	COLOR	
	PIN TYPE I	PIN TYPE II
1	Blue	White
2	Orange	White
3	Green	White
4	Brown	White
5	Gray	White
6	Blue	Red
7	Orange	Red
8	Green	Red
9	Brown	Red
10	Gray	Red
11	Blue	Black
12	Orange	Black
13	Green	Black
14	Brown	Black
15	Gray	Black
16	Blue	Yellow
17	Orange	Yellow
18	Green	Yellow
19	Brown	Yellow
20	Gray	Yellow
21	Blue	Purple
22	Orange	Purple
23	Green	Purple
24	Brown	Purple
25	Gray	Purple

## Telco-50 CAT.3 Structure

**Table 192** Telco-50 Cable Structure

WIRE DIAMETER (MM)	NUMBER OF PAIRS (P)	INSULATION THICKNESS (MM)	CABLE DIAMETER (MM)	ALUMINUM STRIP LAMINATE THICKNESS (MM)	OUTER SHEATH THICKNESS (MM)	FINAL DIAMETER OF THE ROUND CABLE (MM)
0.50	25	0.2	9.7	-	1.0	11.8 <sup>±</sup> 1.0

**Figure 249** Telco-50 Cable Structure

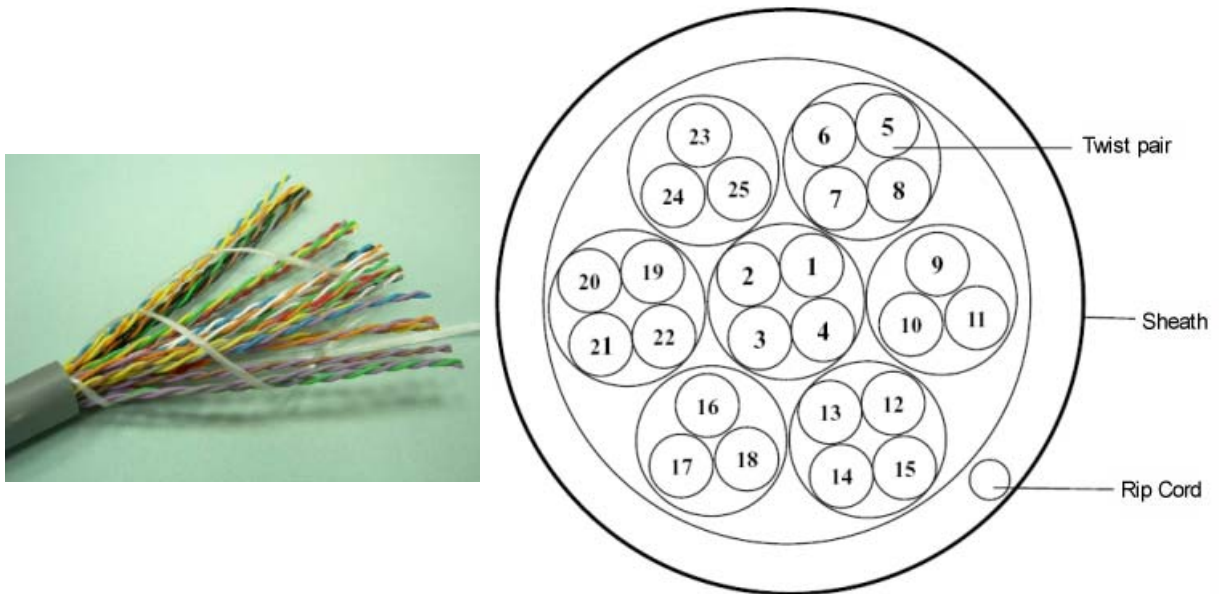


### Telco-50 CAT.5 Structure

**Table 193** Telco-50 Cable Structure

WIRE DIAMETER (MM)	NUMBER OF PAIRS (P)	INSULATION THICKNESS (MM)	CABLE DIAMETER (MM)	ALUMINUM STRIP LAMINATE THICKNESS (MM)	OUTER SHEATH THICKNESS (MM)	FINAL DIAMETER OF THE ROUND CABLE (MM)
0.515	25	0.2	11.0	-	1.0	13.0 <sup>±</sup> 1.0

**Figure 250** Telco-50 Cable Structure



## Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 194** Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

**Table 194** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.

**Table 194** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.





# Legal Information

## Copyright

Copyright © 2013 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

### FCC Warning

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

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

### CE Mark Warning:

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

### Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

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

### Viewing Certifications

- Go to <http://www.zyxel.com>.
- Select your product on the ZyXEL home page to go to that product's page.
- Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

### Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Use ONLY power wires of the appropriate wire gauge (see [Chapter 47 on page 381](#) for details) for your device. Connect it to a power supply of the correct voltage (see [Chapter 47 on page 381](#) for details).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The length of exposed (bare) power wire should not exceed 7 mm.
- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication lines cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using these products (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.
- Do not use the device outside, and make sure all the connections are indoors. There may be a remote risk of electric shock from lightning.
- The RJ-45 jacks are not used for telephone line connection.
- CLASS 1 LASER PRODUCT
- APPAREIL A LASER DE CLASS 1
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.
- To protect yourself from the Device's high operating temperature, wear protective gloves before you touch the Device.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



# Index

## Numbers

- 802.1P priority [83](#)
- 802.3x flow control [83](#)

## A

- AAA server [236](#)
- access control
  - limitations [334](#)
  - login account [344](#)
  - remote management [354](#)
  - service port [353](#)
  - SNMP [334](#)
- activating upstream band 0 [108](#)
- actual aggregate Tx power [362](#)
- adding noise level [116](#)
- address learning, MAC [139](#)
- Address Resolution Protocol (ARP) [367](#)
- administrator login account [344](#)
- ADSL band [99](#)
- ADSL2 and ADSL 2+ band [99](#)
- age setting for MSTP [172](#)
- aggregator ID [182, 183](#)
- aging time of MAC address table [75](#)
- Alarm port pin assignments [392](#)
- ALM LED [31](#)
- amount of transmission output power [362](#)
- Annex A [98, 107](#)
- application [19](#)
  - curbside [20](#)
  - MTU [19](#)
- ARP
  - how it works [367](#)
- ARP (Address Resolution Protocol) [367](#)
- ARP inspection [249, 251](#)
  - and MAC filter [252](#)
  - configuring [252](#)
  - syslog messages [252](#)

- trusted ports [252](#)
- ARP table
  - viewing [367](#)
- attainable net data rate [362](#)
- authentication [236](#)
  - setup [242](#)
- authorization [236](#)
  - privilege levels [242](#)
- auto-crossover [28](#)
- automatic VLAN registration [130](#)

## B

- back up, configuration file [330](#)
- basic settings of the device [70](#)
- basic setup tutorial [46](#)
- binding [249](#)
- binding table [249](#)
  - building [249](#)
- bitstamp [107](#)
- BPDU [161](#)
- Bridge Protocol Data Unit, see BPDU
- broadcast storm control [176](#)

## C

- CDP [284](#)
- certifications [401](#)
  - notices [401](#)
  - viewing [401](#)
- CFI (Canonical Format Indicator) [129](#)
- CFM
  - actions [370](#)
  - CC [274](#)
  - CFM,how it works [274](#)
  - Connectivity Check [274](#)
  - Connectivity Fault [274](#)
  - link trace test [275](#)

- loopback test [275](#)
- MA [274, 275](#)
- MD [274, 277](#)
  - level [277](#)
- MEP [274](#)
- MIP [274](#)
- Test Report [371](#)
- changing administrator password [39](#)
- channel 1 [104](#)
- channel for VDSL transmission statistics exchange [107](#)
- channel transfer function [362](#)
- Cisco Discovery Protocol, see CDP
- CIST [164](#)
- class mask in VDSL [107](#)
- Class of Service (CoS) [304](#)
- classifier [194, 197](#)
  - and QoS [194](#)
  - editing [197](#)
  - example [199](#)
  - overview [194](#)
  - setup [194, 197](#)
  - viewing [197](#)
- code violation [125](#)
- Common and Internal Spanning Tree, see CIST
- configuration [303](#)
  - changing running config [331](#)
  - file names [331](#)
  - saving [39](#)
- configuration file [40](#)
  - backup [330](#)
  - restore [40, 329](#)
  - saving [331](#)
  - uploading through console [40](#)
- configured vs. actual VDSL rate [98](#)
- configuring primary and fallback VDSL templates [103](#)
- configuring primary and fallback VDSL templates for ports [103](#)
- configuring VDSL alarm template for ports [103](#)
- configuring VDSL templates [104](#)
- console cable pin assignments [391](#)
- console port [26](#)
  - settings [30](#)
- copper wire [97](#)
- copyright [401](#)
- CPU [369](#)

- CPU management port [146](#)
- CRC (Cyclic Redundant Check) [69](#)
- current date [73](#)
- current time [73](#)

## D

- daylight saving time [73](#)
- default Ethernet settings [27](#)
- default IP address [30](#)
- DELTA [54, 361](#)
  - actual aggregate Tx power [362](#)
  - attainable net data rate [362](#)
  - line attenuation (LATN) [362](#)
  - signal attenuation (SATN) [362](#)
  - Signal-to-Noise Ratio Margin [362](#)
- desktop installation procedure [23, 25](#)
- destination lookup failure (DLF) [176](#)
- DHCP [311](#)
  - configuration options [311](#)
  - modes [311](#)
  - relay agent [311](#)
  - relay example [320](#)
  - setup [318](#)
- DHCP relay option 82 [251](#)
- DHCP snooping [249](#)
  - configuring [251](#)
  - DHCP relay option 82 [251](#)
  - trusted ports [250](#)
  - untrusted ports [250](#)
- DHCP snooping database [250](#)
- DHCPv6 relay [321, 324](#)
- diagnostics [356](#)
  - ping [356](#)
  - port test [357](#)
  - system log [356](#)
- Differentiated Service (DiffServ) [304](#)
- DiffServ [304](#)
  - activate [306](#)
  - and TRTCM [308](#)
  - DS field [304](#)
  - DSCP [304](#)
  - DSCP-to-IEEE802.1p mapping [309](#)
  - network example [304](#)
  - PHB [304](#)

DiffServ Code Point (DSCP) [304](#)  
 dimensions [384](#)  
 disclaimer [401](#)  
 Discrete Multi-Tone, see DMT  
 distance checking to CPE [363](#)  
 distance to CPE [364](#)  
 DMT [98](#)  
 documentation  
   related [2](#)  
 double-tagged frames [208](#)  
 down-shift SNR margin [110](#)  
 down-shift time [110](#)  
 Downstream Power Back Off (DPBO) [99](#)  
 DPBO [99](#)  
   Electrical Length [100](#)  
 DS (Differentiated Services) [304](#)  
 DSCP  
   DSCP-to-IEEE802.1p mapping [309](#)  
   service level [304](#)  
   what it does [304](#)  
 dual firmware [328](#)  
 Dual-End Loop Test, see DELT  
 Dual-End-Loop-Test [54](#)  
 Dynamic Host Configuration Protocol, see DHCP  
 dynamic link aggregation [180](#)

## E

egress port [149](#)  
 EIA standard size [24](#)  
 Errored Seconds (ES) [123](#)  
 estimated attenuation [364](#)  
 estimated delays [364](#)  
 estimated errors [364](#)  
 Ethernet broadcast address [367](#)  
 Ethernet cable pin assignments [393](#)  
 Ethernet port details [67](#)  
 example  
   MIP and MEP [275](#)  
   primary and fallback VDSL template settings [102](#)  
   VDSL profile settings [101](#)  
 external authentication server [237](#)

## F

fallback VDSL template [102](#)  
 fan speed [72](#)  
 far-end crosstalk [99](#)  
 far-end crosstalk (FEXT) [107](#)  
 FCC interference statement [401](#)  
 file transfer using FTP  
   command example [332](#)  
 filename convention, configuration [331](#)  
 filtering [158](#)  
   rules [158](#)  
 filtering database, MAC table [365](#)  
 fine tune Limit PSD Mask [108](#)  
 firmware [71](#)  
   check firmware index [329](#)  
   select firmware index [328](#)  
   upgrade [328](#)  
 flow control [83](#)  
   back pressure [83](#)  
   IEEE 802.3x [83](#)  
 following the North American VDSL2 standard [107](#)  
 Forward Error Correction Seconds (FECS) [123](#)  
 forwarding  
   delay [172](#)  
 frames  
   tagged [138](#)  
   untagged [138](#)  
 front panel [26](#)  
 FTP [331](#)  
   file transfer procedure [332](#)  
   restrictions over WAN [333](#)  
 FTP for management [21](#)

## G

G.993.2 [97, 107](#)  
 G.997.1 [100](#)  
 GARP [130](#)  
 GARP terminology [130](#)  
 GARP timer [75, 130](#)  
 gauge of telephone wire [364](#)  
 general setup [72](#)  
 Generic Attribute Registration Protocol, see GARP

getting help [41](#)  
 getting VDSL transmission statistics [107](#)  
 Gigabit ports [27](#)  
 GMT (Greenwich Mean Time) [73](#)  
 GVRP [130, 137, 138](#)  
   and port assignment [138](#)  
 GVRP (GARP VLAN Registration Protocol) [130](#)

## H

Handshake status [54](#)  
 hardware alarm profile [87](#)  
 hardware installation [23](#)  
 hardware monitor [71](#)  
 hardware overview [26](#)  
 hello time [172](#)  
 Hlin [362](#)  
 Hlog [362](#)  
 hops [172](#)  
 HTTPS [347](#)  
   certificates [347](#)  
   implementation [347](#)  
   public keys, private keys [347](#)  
 HTTPS example [348](#)  
 humidity of operating environment [384](#)  
 humidity of storage environment [384](#)

## I

IAT [119](#)  
 IEEE 802.1p, priority [76](#)  
 IEEE 802.1x  
   activate [188, 189, 240, 242](#)  
   port authentication [186](#)  
   reauthentication [189](#)  
 IGMP  
   version [217](#)  
 IGMP (Internet Group Management Protocol) [217](#)  
 IGMP filtering [217](#)  
   profile [227](#)  
   profiles [224](#)  
 IGMP per port counter [221, 222](#)  
 IGMP snooping [217](#)  
   and VLANs [218](#)  
   MVR [229](#)  
   setup [226](#)  
 Impulse Noise Monitoring, see INM  
 Impulse Noise Protection (INP) [98](#)  
 incorrect cyclic redundancy check [125](#)  
 ingress port [149](#)  
 INM [119](#)  
   cluster [119](#)  
   cluster continuation [119](#)  
   Eq INP [119](#)  
   equivalent INP, see Eq INP  
   gap [119](#)  
   histogram [119](#)  
   IAT Offset [121](#)  
   IAT Step [121](#)  
   INMCC [119, 120](#)  
 INM cluster continuation, see INMCC  
 INP [98](#)  
 installation  
   desktop [23, 25](#)  
   mini-GBIC transceivers [28](#)  
   precautions [24](#)  
   rack-mounting [24](#)  
 installation scenarios [23](#)  
 Inter-Arrival Time, see IAT  
 Internet Protocol version 6 [76](#)  
 introduction [19](#)  
 IP address [80](#)  
 IP interface [79](#)  
 IP setup [79](#)  
 IP source guard [249](#)  
   ARP inspection [249, 251](#)  
   DHCP snooping [249](#)  
   static bindings [249](#)  
 IP subnet mask [80](#)  
 IPv6 [76](#)  
   addressing [76](#)  
   EUI-64 [78](#)  
   global address [77](#)  
   global ID [78](#)  
   interface ID [77](#)  
   link-local address [77](#)  
   MLD [218](#)  
   neighbor cache [373](#)  
   prefix [77](#)

- prefix length [77](#)
  - route list [374](#)
  - stateless autoconfiguration [78](#)
  - subnet ID [78](#)
  - unspecified address [78](#)
  - IPv6 cache
    - introduction [372](#)
    - messages types [372](#)
    - packet transmission [372](#)
  - ISDD Sensitivity [121](#)
  - ISDN frequency range [99](#)
- ## L
- L2PT [282](#)
    - access port [283](#)
    - CDP [282](#)
    - configuration [284](#)
    - encapsulation [282](#)
    - LACP [283](#)
    - MAC address [282](#)
    - mode [283](#)
    - overview [282](#)
    - PAgP [283](#)
    - point to point [283](#)
    - STP [282](#)
    - tunnel port [283](#)
    - UDLD [283](#)
    - VTP [282](#)
  - LACP [180, 285](#)
    - system priority [183](#)
    - timeout [184](#)
  - LATN [362](#)
  - Layer 2 protocol tunneling, see L2PT
  - LD\_Done status [54](#)
  - LD\_Test status [54](#)
  - LEDs [31](#)
    - ALM [31](#)
    - PWR [31](#)
    - SYS [31](#)
  - limit mask in VDSL [107](#)
  - Limit PSD Mask [107](#)
    - fine tune [108](#)
  - limiting broadcast, multicast, DLF packets [176](#)
  - line attenuation [362](#)
  - Link Aggregate Control Protocol (LACP) [180](#)
  - link aggregation [180](#)
    - dynamic [180](#)
    - ID information [181](#)
    - setup [182, 183](#)
    - status [181](#)
  - link trace [275](#)
  - lockout [39](#)
  - login [33](#)
    - password [39](#)
  - login account
    - administrator [344](#)
    - non-administrator [345](#)
  - login accounts [344](#)
    - configuring via Web Configurator [344](#)
    - multiple [344](#)
    - number of [344](#)
  - login password [345](#)
  - loop diagnostic [361, 362, 363, 371](#)
    - test [361](#)
  - loop guard [270](#)
    - examples [271](#)
    - port shut down [272](#)
    - setup [272](#)
    - vs. STP [270](#)
  - loop length [364](#)
  - loop test [361](#)
  - loop type [364](#)
  - loopback test [275](#)
  - Loss Of Framing Seconds (LOFS) [123](#)
  - Loss of Power Seconds (LPRS) [123](#)
  - Loss Of Signals Seconds (LOSS) [123](#)
- ## M
- MA [275](#)
  - MA VLAN ID [276](#)
  - MAC (Media Access Control) [71](#)
  - MAC address [71, 367](#)
  - MAC address learning [75, 139](#)
  - MAC authentication [186](#)
    - aging time [190](#)
    - example [187](#)
    - setup [189](#)
  - MAC based VLANs [144](#)

- MAC filter
  - and ARP inspection [252](#)
- MAC limit [191](#)
  - port security [192](#)
  - VLAN security [192](#)
- MAC table [365](#)
  - how it works [365](#)
  - viewing [366](#)
- maintenance [327](#)
  - configuration backup [330](#)
  - current configuration [327](#)
  - firmware [328](#)
  - main screen [327](#)
  - restoring configuration [329](#)
- Maintenance Association (MA) [274](#)
- Maintenance Domain (MD) [274](#)
- Maintenance End Point (MEP) [274](#)
- Maintenance Intermediate Point (MIP) [274](#)
- Management Information Base (MIB) [335](#)
- management port [29, 149](#)
  - default IP address [30](#)
- managing the device
  - good habits [21](#)
  - using FTP [21](#)
  - using Telnet. See command interface. [21](#)
  - using the command interface. See command interface. [21](#)
- man-in-the-middle attacks [251](#)
- max
  - hops [172](#)
- MD [277](#)
- MD level [275](#)
- MDIX (Media Dependent Interface Crossover) [28](#)
- memory [369](#)
- MGMT port [29](#)
- MIB
  - and SNMP [335](#)
  - supported MIBs [336](#)
- MIB (Management Information Base) [335](#)
- MIB PSD MASK [108](#)
- MIB PSD Mask [111](#)
  - graph [111](#)
- mini-GBIC transceivers [28](#)
  - installation [28](#)
  - MultiSource Agreement [28](#)
  - removal [29](#)
- MIP and MEP example [275](#)
- mirroring ports [178](#)
- MLD filtering [218](#)
- MLD message [218](#)
- MLD proxy [218](#)
- MLD snooping [218](#)
- mode of power management [107](#)
- monitor port [178, 179](#)
- mounting brackets [24](#)
- MRSTP status [170](#)
- MST ID [164](#)
- MST Instance, see MSTI
- MST region [163](#)
- MSTI [164](#)
- MSTP [160, 162](#)
  - bridge ID [174, 175](#)
  - configuration [171](#)
  - configuration digest [175](#)
  - forwarding delay [172](#)
  - Hello Time [174](#)
  - hello time [172](#)
  - Max Age [174](#)
  - max hops [172](#)
  - maximum age for MSTP [172](#)
  - path cost [173](#)
  - port priority [173](#)
  - revision level [172](#)
  - status [173](#)
- MTU [19](#)
- MTU (Multi-Tenant Unit) [74](#)
- multicast [217](#)
  - 802.1 priority [224](#)
  - and IGMP [217](#)
  - IP addresses [217](#)
  - overview [217](#)
  - setup [224](#)
- multicast group [227](#)
- Multicast Listener Discovery [218](#)
- multicast VLAN [232](#)
- multiple login accounts [344](#)
- Multiple Rapid Spanning Tree Protocol [162](#)
- Multiple RSTP [162](#)
- Multiple Spanning Tree Protocol, See MSTP [162](#)
- Multiple Spanning Tree Protocol, see MSTP
- Multiple STP [162](#)
- Multiple Tenant Unit, see MTU



MultiSource Agreement (MSA) [28](#)  
 mutlicast traffic statistics [221, 222](#)  
 MVR [229](#)  
   configuration [230](#)  
   group configuration [232](#)  
   network example [229](#)  
 MVR (Multicast VLAN Registration) [229](#)

## N

NDP [372](#)  
 neighbor advertisement [372](#)  
 Neighbor Discovery Protocol, see NDP  
 neighbor solicitation [372](#)  
 network applications [19](#)  
 network management system (NMS) [334](#)  
 non-administrator login account [345](#)  
 note  
   DC power connection [384](#)  
 note for SELT [364](#)  
 NTP (RFC-1305) [73](#)  
 number of VDSL templates [104](#)

## O

open loop [364](#)  
 optical fiber [97](#)  
 other documentation [2](#)  
 overhead channel [107](#)

## P

packet buffer [369](#)  
 PAE PVC [299](#)  
 PAGP [285](#)  
 password [39](#)  
 password change for administrator [39](#)  
 PHB (Per-Hop Behavior) [304](#)  
 PhyR [117](#)  
 pin assignment  
   console cable [391](#)

Ethernet cable [393](#)  
 ping, test connection [356](#)  
 policy [202](#)  
   and classifier [202](#)  
   and DiffServ [200](#)  
   configuration [202](#)  
   example [204](#)  
   overview [200](#)  
   rules [200](#)  
 Port Aggregation Protocol, see PAGP  
 port authentication [186](#)  
   and RADIUS [237](#)  
   IEEE802.1x [188, 240, 242](#)  
   MAC authentication [186](#)  
 port based VLAN type [75](#)  
 port based VLANs [146](#)  
 port isolation [137, 149](#)  
 port mirroring [178, 179](#)  
   direction [179](#)  
   egress [179](#)  
   ingress [179](#)  
 port redundancy [180](#)  
 port security  
   setup [272, 284](#)  
 port setup [82](#)  
 port status [53](#)  
 port test [357](#)  
 port VLAN ID, see PVID  
 port VLAN trunking [131](#)  
 port-based VLAN  
   all connected [149](#)  
   port isolation [149](#)  
   settings wizard [149](#)  
 ports  
   "standby" [180](#)  
   mirroring [178](#)  
   speed/duplex [83](#)  
 power connection  
   warning [27](#)  
 power connector [26](#)  
 power consumption [384](#)  
 power management [107](#)  
 power specification [384](#)  
 Power Spectral Density, see PSD  
 power status [72](#)  
 power voltage [72](#)

PPPoE IA  
   circuit ID [289](#)  
   configuration [289](#)  
   overview [288](#)  
   remote ID [289](#)  
   status [290](#)  
   sub-option [289](#)  
   tag format [288](#)  
   WT-101 [289](#)

PPPoE Intermediate Agent, see PPPoE IA [288](#)

primary and fallback VDSL template example [102](#)

primary VDSL template [102](#)

priority level [76](#)

priority, queue assignment [76](#)

privilege setting for users [345](#)

product registration [402](#)

profile  
   VDSL line [101](#)

protocol based VLAN [141](#)  
   and IEEE 802.1Q tagging [141](#)  
   example [143](#)  
   hexadecimal notation for protocols [143, 145](#)  
   isolate traffic [141](#)  
   priority [143, 145](#)

protocol for STP [161](#)

PSD [97](#)

PVC configuration [295](#)

PVID [129, 137](#)

PWR LED [31](#)

## Q

QLN [362](#)

QoS  
   and classifier [194](#)

queue weight [205](#)

queuing [205](#)  
   SPQ [205](#)  
   WRR [205](#)

queuing method [205, 207](#)

Quiet Line Noise, see QLN

## R

rack-mounting [24](#)  
   precautions [24](#)  
   screwdriver type [24](#)  
   screws type [24](#)

rack-mounting kit [24](#)

Radio Frequency Interference, see RFI

RADIUS [237](#)  
   advantages [237](#)  
   and port authentication [237](#)  
   and tunnel protocol attribute [245](#)  
   Network example [236](#)  
   server [237](#)  
   settings [237](#)  
   setup [237](#)

Rapid Spanning Tree Protocol, see RSTP

rate adaption [100](#)  
   dynamic mode [110](#)  
   rate adaptive at initial mode [110](#)

rate adaption ratio [104](#)

rate adaptive [108](#)

rate adaptive at initial mode [110](#)

rate adaptive dynamic changing mode [110](#)

rate limit profile [84, 85](#)

read-only access  
   non-administrator [345](#)

real length to Electrical Length calculation [100](#)

rear panel connections [26](#)

reboot  
   load configuration [331](#)

reboot system [331](#)

receiving power [107](#)

reflections [364](#)

registration  
   product [402](#)

related documentation [2](#)

relationships of VDSL template, line profiles,  
   channel profiles, and ports [101](#)

remote management [354](#)  
   service [355](#)  
   trusted computers [355](#)

resetting [40, 330](#)  
   to factory default settings [330](#)

restoring configuration [40, 329](#)

RFC 3164 [358](#)

RFI [101](#)  
 RFI band [108](#)  
 Round Robin Scheduling [205](#)  
 router advertisement [372](#)  
 router solicitation [372](#)  
 RSTP [160](#)  
 rubber feet [23](#)

## S

safety certifications [387](#)  
 safety warnings [402](#)  
 SATN [362](#)  
 save configuration [331](#)  
 saving configuration [39](#)  
 screwdriver type [24](#)  
 screws [24](#)  
 Secure Shell, see SSH  
 SELT [363](#)

- estimated delays [364](#)
- estimated errors [364](#)
- loop length [364](#)
- reflections [364](#)
- termination [364](#)

 service access control [353](#)

- service port [354](#)

 Severely Errored Seconds (SES) [123](#)  
 SFP [28](#)  
 Showtime status [54](#)  
 signal attenuation [362](#)  
 signal echoes [364](#)  
 Signal to Noise Ratio, see SNR  
 Signal-to-Noise Ratio Margin [362](#)  
 Signal-to-Noise Ratio, see SNR  
 Simple Network Management Protocol, see  
 SNMP [334](#)  
 Single-End Loop Test, see SELT  
 Small Form-factor Pluggable, see SFP  
 SNMP [334](#)

- agent [335](#)
- and MIB [335](#)
- and security [335](#)
- authentication [343](#)
- communities [343](#)

- management model [335](#)
- manager [335](#)
- MIB [336](#)
- network components [335](#)
- object variables [335](#)
- protocol operations [335](#)
- security [343](#)
- setup [342, 344](#)
- version 3 [335](#)
- versions supported [334](#)

 SNMP trap group [344](#)  
 SNMP traps [336](#)

- authentication [340](#)
- autonegotiation [338](#)
- coldstart [336](#)
- externalarm [337](#)
- fanspeed [337](#)
- linkdown [338](#)
- linkup [338](#)
- loopguard [337](#)
- mactable [341](#)
- reset [337](#)
- rmon [341](#)
- setup [344](#)
- SFP [338](#)
- stp [340](#)
- temperature [337](#)
- voltage [337](#)
- warmstart [336](#)

 SNR [100, 107](#)  
 SNRM [362](#)  
 specification [104](#)  
 SSH [346](#)

- encryption methods [347](#)
- how SSH works [346](#)
- implementation [347](#)

 SSL (Secure Socket Layer) [347](#)  
 standby ports [180](#)  
 static bindings [249](#)  
 static link aggregation example [184](#)  
 static MAC address [152](#)  
 static MAC forwarding [139, 152](#)  
 static multicast address [154](#)  
 static multicast forwarding [154](#)  
 static routes [303](#)  
 static trunking example [184](#)  
 Static VLAN [134](#)

- static VLAN
    - control [135](#)
    - tagging [135](#)
  - status [34, 53](#)
    - Ethernet port details [67](#)
    - link aggregation [181](#)
    - MSTP [173](#)
    - port [53](#)
    - power [72](#)
    - STP [167, 170](#)
    - VLAN [132](#)
    - VLAN port detail [55](#)
  - storing user profiles [236](#)
  - STP [160, 285](#)
    - bridge ID [168, 170](#)
    - bridge priority [166, 169](#)
    - configuration [166, 168](#)
    - designated bridge [161](#)
    - forwarding delay [167, 169](#)
    - Hello BPDU [161](#)
    - Hello Time [166, 168, 169, 170](#)
    - how it works [161](#)
    - Max Age [166, 168, 169, 170](#)
    - path cost [160, 167, 169](#)
    - port priority [167, 169](#)
    - port state [161](#)
    - root port [161](#)
    - status [167, 170](#)
    - terminology [160](#)
    - vs. loop guard [270](#)
  - Strict Priority Queuing, see SPO
  - sub-channel of a VDSL band [113](#)
  - subnet based VLAN [140](#)
    - and DHCP VLAN [140](#)
    - priority [140](#)
    - setup [139](#)
  - subnet based VLANs [138](#)
  - switch lockout [39](#)
  - switch setup [75](#)
  - SYS LED [31](#)
  - syslog [252, 358](#)
    - protocol [358](#)
    - server setup [360](#)
    - settings [359](#)
    - setup [359](#)
    - severity levels [358](#)
  - system information [70](#)
  - system log [356](#)
  - system reboot [331](#)
  - system reset [40](#)
- ## T
- TACACS+ [237](#)
    - setup [240](#)
  - TACACS+ (Terminal Access Controller Access-Control System Plus) [236](#)
  - Tag Protocol Identifier, see TPID
  - tagged VLAN [129](#)
  - Telco-50 connector pin assignments [388](#)
  - temperature indicator [71](#)
  - temperature of operating environment [384](#)
  - temperature of storage environment [384](#)
  - terminal emulation [30](#)
  - threshold before xDSL rate adjustment [110](#)
  - thresholds for hardware alarm [87](#)
  - time
    - current [73](#)
    - time zone [73](#)
  - Time (RFC-868) [73](#)
  - time server [73](#)
  - time service protocol [73](#)
    - format [73](#)
  - tone [113](#)
    - frequency width [113](#)
  - TPID [210](#)
  - trademarks [401](#)
  - Training status [54](#)
  - transceivers of mini-GBIC [28](#)
    - installation [28](#)
    - removal [29](#)
  - transmission mode in VDSL [107](#)
  - transmission power [107](#)
  - trap group [344](#)
  - traps
    - destination [343](#)
  - troubleshooting for DHCP relay tutorial [50](#)
  - TRTCM
    - and bandwidth control [308](#)
    - and DiffServ [308](#)
    - color-aware mode [306](#)
    - color-blind mode [306](#)

- setup [307](#)
- trunk group [180](#)
- trunking [180](#)
  - example [184](#)
- trusted ports
  - ARP inspection [252](#)
  - DHCP snooping [250](#)
- tunnel protocol attribute, and RADIUS [245](#)
- tutorials [46](#)
- Two Rate Three Color Marker (TRTCM) [305](#)
- Type of Service (ToS) [304](#)

## U

- UDLD [285](#)
- UnAvailable Seconds (UAS) [123](#)
- UniDirectional Link Detection, see UDLD
- untrusted ports
  - ARP inspection [252](#)
  - DHCP snooping [250](#)
- UPBO [98](#)
  - Electrical Length [100](#)
  - variable A and B [107](#)
- up-shift SNR margin [110](#)
- up-shift time [110](#)
- upstream band 0, see US0
- Upstream Power Back Off, see UPBO
- US0 [108](#)
- US0 mask in VDSL [107](#)
- user profiles storing [236](#)

## V

- VDSL
  - Limit PSD Mask [97](#)
- VDSL alarm profile [121](#)
- VDSL channel alarm profile [122](#)
- VDSL channel profile [104](#)
  - PhyR [117](#)
- VDSL INM profile [119](#)
- VDSL line alarm profile [122](#)
- VDSL line profile [104](#)

- bits and power reallocation [107](#)
- class mask [107](#)
- down-shift SNR margin [110](#)
- down-shift time [110](#)
- DPBO [112](#)
- limit mask [107](#)
- overhead rate [107](#)
- receiving power [107](#)
- RFI band [108, 113](#)
- transmission mode [107](#)
- transmission power [107](#)
- up-shift SNR margin [110](#)
- up-shift time [110](#)
- US0 mask [107](#)
- Virtual Noise [108, 115](#)
- VDSL port
  - configuring primary and fallback VDSL templates [103](#)
  - configuring VDSL alarm template [103](#)
- VDSL port detail [55](#)
- VDSL port status
  - Handshake [54](#)
  - LD\_Done [54](#)
  - LD\_Test [54](#)
  - Showtime [54](#)
  - Training [54](#)
- VDSL profile setting example [101](#)
- VDSL template
  - rate adaption ratio [104](#)
- VDSL template settings [104](#)
- VDSL2 [97](#)
- VDSL2 profiles [98](#)
- Vendor Specific Attribute, see VSA
- ventilation [23](#)
- ventilation holes [24](#)
- Very High Speed Digital Subscriber Line 2, see VDSL2
- VID [129, 132, 133, 210](#)
  - number of possible VIDs [129](#)
  - priority frame [129](#)
- viewing hardware information [369](#)
- viewing maximum transmission data rate [362](#)
- viewing xDSL sub-carrier status [362](#)
- Virtual Noise [108, 115](#)
- VLAN [74, 129](#)
  - acceptable frame type [138](#)
  - automatic registration [130](#)

- ID [129](#)
- IGMP snooping [218](#)
- ingress filtering [137](#)
- introduction [74](#)
- MAC based [144](#)
- number of VLANs [132](#)
- port based [146](#)
- port isolation [137](#)
- port number [133](#)
- port settings [137](#)
- port-based, all connected [149](#)
- port-based, isolation [149](#)
- port-based, wizard [149](#)
- static VLAN [134](#)
- status [132](#), [133](#)
- subnet based [138](#)
- tagged [129](#)
- trunking [131](#), [138](#)
- type [75](#), [131](#)
- VLAN (Virtual Local Area Network) [74](#)
- VLAN ID [80](#), [89](#)
- VLAN Identifier, see VID
- VLAN mapping [278](#)
  - activating [279](#)
  - configuration [280](#)
  - example [278](#)
  - priority level [278](#)
  - tagged [278](#)
  - traffic flow [278](#)
  - untagged [278](#)
  - VLAN ID [278](#)
- VLAN profile [101](#)
- VLAN stacking [208](#)
  - configuration [211](#)
  - example [208](#)
  - frame format [210](#)
  - port roles [209](#), [212](#)
  - port-based inner Q [215](#)
  - port-based Q-in-Q [212](#)
  - priority [210](#)
  - selective Q-in-Q [214](#)
  - TPID [210](#)
  - Tunnel TPID [210](#)
  - VLAN tag format [210](#)
- VLAN tag format [210](#)
- VLAN Trunking Protocol, see VTP
- VLAN, protocol based, see protocol based VLAN
- VSA [244](#)

- VT100 [30](#)
- VTP [285](#)
- VTUC [125](#)
- VTUR [125](#)

## W

- warning for power connection [27](#)
- warranty [401](#)
  - note [402](#)
- web configurator [33](#)
  - getting help [41](#)
  - home [34](#)
  - login [33](#)
  - logout [41](#)
  - navigation panel [36](#)
- weight, queuing [205](#)
- Weighted Round Robin Scheduling, see WRR
- WRR [205](#)

## Z

- ZyNOS (ZyXEL Network Operating System) [332](#)