GS3700/ XGS3700 Series

GbE L2+ Switch

Version 4.30
Edition 1, 10/2015

User's Guide

Default Login Details	
IP Address	http://192.168.0.1 (Out-of-band MGMT port) http://192.168.1.1 (In-band ports)
User Name	admin
Password	1234

Copyright © 2015 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Note: This guide is a reference for a series of products. Therefore some features or options in this guide may not be available in your product.

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

- CLI Reference Guide

  This guide explains how to use the Command-Line Interface (CLI) to configure the Switch.

Note: It is recommended you use the Web Configurator to configure the Switch.

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

- More Information

  Go to **support.zyxel.com** to find other information on the Switch.

Contents Overview

User's Guide 20

Getting to Know Your Switch 21
Hardware Installation and Connection 26
Hardware Overview 30
The Web Configurator 37

Technical Reference 46

ZON Utility, ZON Neighbor Management and Port Status 47
Basic Setting 56
VLAN 101
Static MAC Forward Setup 124
Static Multicast Forward Setup 127
Filtering 130
Spanning Tree Protocol 132
Bandwidth Control 157
Broadcast Storm Control 160
Mirroring 162
Link Aggregation 175
Port Authentication 185
Port Security 195
Time Range 199
Classifier 201
Policy Rule 210
Queuing Method 215
VLAN Stacking 219
Multicast 227
AAA 253
IP Source Guard 265
Loop Guard 299
VLAN Mapping 303
Layer 2 Protocol Tunneling 307
sFlow 312
PPPoE 316
Error Disable 325
MAC Pinning 333
Private VLAN 336
Green Ethernet 340
Link Layer Discovery Protocol (LLDP) 343

Anti-Arpscan 372
BPDU Guard 378
OAM 381
ZULD 390
Static Route 396
Policy Routing 400
Differentiated Services 404
DHCP 413
VRRP 430
Load Sharing 439
ARP Setup 441
Maintenance 447
Access Control 458
Diagnostic 482
System Log 485
Syslog Setup 486
Cluster Management 489
MAC Table 495
IP Table 498
ARP Table 500
Routing Table 502
Path MTU Table 503
Configure Clone 504
IPv6 Neighbor Table 508
Troubleshooting 510

Table of Contents

Contents Overview 3

Table of Contents 5

Part I: User's Guide 20

Chapter 1
Getting to Know Your Switch 21

1.1 Introduction 21
1.1.1 Bridging Example 22
1.1.2 High Performance Switching Example 22
1.1.3 Gigabit Ethernet to the Desktop 23
1.1.4 IEEE 802.1Q VLAN Application Example 23
1.1.5 IPv6 Support 24
1.2 Ways to Manage the Switch 24
1.3 Good Habits for Managing the Switch 25

Chapter 2
Hardware Installation and Connection 26

2.1 Freestanding Installation 26
2.2 Mounting the Switch on a Rack 27
2.3 Installation Requirements 27
2.3.1 Precautions 27
2.4 Attaching the Brackets to the Switch 27
2.5 Mounting the Switch on a Rack 28
2.6 Power Module Installation 29

Chapter 3
Hardware Overview 30

3.1 Front Panel Connections 30
3.1.1 Ethernet Ports 31
3.1.2 SFP/SFP+ Slots 32
3.1.3 Management Port 33
3.1.4 Console Port 33
3.2 Rear Panel 34
3.2.1 Removing and Installing the Fan Module 34
3.2.2 Power Connection 34
3.3 LEDs 35

Chapter 4
The Web Configurator 37

4.1 Introduction 37
4.2 System Login 37
4.3 The Web Configurator Layout 38
4.3.1 Change Your Password 42
4.4 Saving Your Configuration 43
4.5 Switch Lockout 43
4.6 Resetting the Switch 44
4.6.1 Reload the Configuration File 44
4.7 Logging Out of the Web Configurator 45
4.8 Help 45

Part II: Technical Reference 46

Chapter 5
ZON Utility, ZON Neighbor Management and Port Status 47

5.1 Overview 47
5.2 Status 47
5.3 ZyXEL One Network (ZON) Utility Screen 49
5.4 ZON Neighbor Management Screen 49
5.5 Port Status 51
5.5.1 Port Details 52

Chapter 6
Basic Setting 56

6.1 System Information 56
6.1.1 System Information Stacking Hardware Monitor 59
6.2 General Setup 61
6.3 Introduction to VLANs 63
6.4 Switch Setup 63
6.5 IP Setup 65
6.5.1 IP Interfaces 65
6.5.2 IP Status Details 66
6.5.3 IP Configuration 67
6.6 Port Setup 69
6.7 PoE 72
6.7.1 PoE Time Range Status 75
6.7.2 PoE Setup 76
6.8 Interface Setup 79
6.9 IPv6 80

6.9.1 IPv6 Interface Status 80
6.9.2 IPv6 Configuration 83
6.9.3 IPv6 Global Setup 83
6.9.4 IPv6 Interface Setup 84
6.9.5 IPv6 Link-Local Address Setup 85
6.9.6 IPv6 Global Address Setup 86
6.9.7 IPv6 Neighbor Discovery Setup 87
6.9.8 IPv6 Router Discovery Setup 88
6.9.9 IPv6 Prefix Setup 89
6.9.10 IPv6 Neighbor Setup 91
6.9.11 DHCPv6 Client Setup 92
6.10 Stacking 93
6.10.1 Stacking Status 94
6.10.2 Stacking Slot 95
6.10.3 Stacking Configuration 97
6.11 DNS 99

Chapter 7
VLAN 101

7.1 Introduction to IEEE 802.1Q Tagged VLANs 101
7.1.1 Forwarding Tagged and Untagged Frames 101
7.2 Automatic VLAN Registration 102
7.2.1 GARP 102
7.2.2 GVRP 102
7.3 Port VLAN Trunking 103
7.4 Select the VLAN Type 103
7.5 802.1Q Static VLAN 103
7.5.1 VLAN Status 104
7.5.2 VLAN Details 105
7.6 Private VLAN Status 106
7.7 VLAN Configuration 106
7.7.1 Configure a Static VLAN 107
7.7.2 Configure VLAN Port Settings 109
7.7.3 Subnet Based VLANs 111
7.7.4 Protocol Based VLANs 114
7.8 Port-based VLAN Setup (Standalone Mode) 117
7.8.1 Configure a Port-based VLAN 117
7.9 Voice VLAN 120
7.10 MAC Based VLAN 122

Chapter 8
Static MAC Forward Setup 124

8.1 Overview 124

8.2 Configuring Static MAC Forwarding 124

Chapter 9
Static Multicast Forward Setup 127

9.1 Static Multicast Forwarding Overview 127
9.2 Configuring Static Multicast Forwarding 128

Chapter 10
Filtering 130

10.1 Configure a Filtering Rule 130

Chapter 11
Spanning Tree Protocol 132

11.1 STP/RSTP Overview 132
11.1.1 STP Terminology 132
11.1.2 How STP Works 133
11.1.3 STP Port States 133
11.1.4 Multiple RSTP 133
11.1.5 Multiple STP 134
11.2 Spanning Tree Protocol Status Screen 136
11.3 Spanning Tree Configuration 137
11.4 Configure Rapid Spanning Tree Protocol 138
11.5 Rapid Spanning Tree Protocol Status 141
11.6 Configure Multiple Rapid Spanning Tree Protocol 142
11.7 Multiple Rapid Spanning Tree Protocol Status 145
11.8 Configure Multiple Spanning Tree Protocol 147
11.8.1 Multiple Spanning Tree Protocol Port Configuration 151
11.9 Multiple Spanning Tree Protocol Status 154

Chapter 12
Bandwidth Control 157

12.1 Bandwidth Control Overview 157
12.1.1 CIR and PIR 157
12.2 Bandwidth Control Setup 157

Chapter 13
Broadcast Storm Control 160

13.1 Broadcast Storm Control Setup 160

Chapter 14
Mirroring 162

14.1 Port Mirroring 162
14.1.1 Local Port Mirroring 165

14.1.2 Remote Port Mirroring 167
14.1.3 Source 168
14.1.4 Destination 170
14.1.5 Connected Port 171

Chapter 15
Link Aggregation 175

15.1 Link Aggregation Overview 175
15.2 Dynamic Link Aggregation 175
15.2.1 Link Aggregation ID 176
15.3 Link Aggregation Status 176
15.4 Link Aggregation Setting 177
15.5 Link Aggregation Control Protocol 180
15.6 Static Trunking Example 183

Chapter 16
Port Authentication 185

16.1 Port Authentication Overview 185
16.1.1 IEEE 802.1x Authentication 185
16.1.2 MAC Authentication 186
16.2 Port Authentication Configuration 187
16.2.1 Activate IEEE 802.1x Security 187
16.2.2 Guest VLAN 189
16.2.3 Activate MAC Authentication 192

Chapter 17
Port Security 195

17.1 About Port Security 195
17.2 Port Security Setup 195
17.3 VLAN MAC Address Limit 197

Chapter 18
Time Range 199

18.1 About Time Range 199
18.2 Time Range Setup 199

Chapter 19
Classifier 201

19.1 About the Classifier and QoS 201
19.2 Classifier Status 201
19.3 Classifier Configuration 202
19.3.1 Viewing and Editing Classifier Configuration 206
19.4 Classifier Global Setting Configuration 207

19.5 Classifier Example 208

Chapter 20
Policy Rule 210

20.1 Policy Rules Overview 210
20.1.1 DiffServ 210
20.1.2 DSCP and Per-Hop Behavior 210
20.2 Configuring Policy Rules 210
20.3 Policy Example 213

Chapter 21
Queuing Method 215

21.1 Queuing Method Overview 215
21.1.1 Strictly Priority 215
21.1.2 Weighted Fair Queuing 215
21.1.3 Weighted Round Robin Scheduling (WRR) 216
21.2 Configuring Queuing 216

Chapter 22
VLAN Stacking 219

22.1 VLAN Stacking Overview 219
22.1.1 VLAN Stacking Example 219
22.2 VLAN Stacking Port Roles 220
22.3 VLAN Tag Format 220
22.3.1 Frame Format 221
22.4 Configuring VLAN Stacking 221
22.4.1 Port-based Q-in-Q 223
22.4.2 Selective Q-in-Q 225

Chapter 23
Multicast 227

23.1 Multicast Overview 227
23.1.1 IP Multicast Addresses 227
23.1.2 IGMP Filtering 227
23.1.3 IGMP Snooping 228
23.1.4 IGMP Snooping and VLANs 228
23.1.5 MLD Snooping-Proxy 228
23.1.6 MLD Messages 229
23.2 Multicast Setup 229
23.3 IPv4 Multicast Status 230
23.3.1 IGMP Snooping 230
23.3.2 IGMP Snooping VLAN 234
23.3.3 IGMP Filtering Profile 235

23.4 IPv6 Multicast Status 236
23.4.1 MLD Snooping-proxy 237
23.4.2 MLD Snooping-proxy VLAN 237
23.4.3 MLD Snooping-proxy VLAN Port Role Setting 239
23.4.4 MLD Snooping-proxy Filtering 241
23.4.5 MLD Snooping-proxy Filtering Profile 243
23.5 MVR Overview 244
23.5.1 Types of MVR Ports 245
23.5.2 MVR Modes 245
23.5.3 How MVR Works 245
23.6 General MVR Configuration 246
23.6.1 MVR Group Configuration 248
23.6.2 MVR Configuration Example 250

Chapter 24
AAA 253

24.1 Authentication, Authorization and Accounting (AAA) 253
24.1.1 Local User Accounts 253
24.1.2 RADIUS and TACACS+ 254
24.2 AAA Screens 254
24.2.1 RADIUS Server Setup 254
24.2.2 TACACS+ Server Setup 256
24.2.3 AAA Setup 257
24.2.4 Vendor Specific Attribute 260
24.2.5 Tunnel Protocol Attribute 261
24.3 Supported RADIUS Attributes 261
24.3.1 Attributes Used for Authentication 262
24.3.2 Attributes Used for Accounting 262

Chapter 25
IP Source Guard 265

25.1 IP Source Guard Overview 265
25.1.1 What You Can Do 265
25.1.2 What You Need to Know 266
25.2 IP Source Guard 267
25.3 IPv4 Source Guard Setup 268
25.4 IPv4 Source Guard Static Binding 269
25.5 DHCP Snooping 271
25.6 DHCP Snooping Configure 273
25.6.1 DHCP Snooping Port Configure 275
25.6.2 DHCP Snooping VLAN Configure 277
25.6.3 DHCP Snooping VLAN Port Configure 278
25.7 ARP Inspection Status 279

25.7.1 ARP Inspection VLAN Status 280
25.7.2 ARP Inspection Log Status 281
25.8 ARP Inspection Configure 282
25.8.1 ARP Inspection Port Configure 284
25.8.2 ARP Inspection VLAN Configure 286
25.9 IPv6 Source Guard Overview 287
25.10 IPv6 Source Binding Status 287
25.11 IPv6 Static Binding Setup 288
25.12 IPv6 Source Guard Policy Setup 290
25.13 IPv6 Source Guard Port Setup 291
25.14 IPv6 Snooping Policy Setup 292
25.15 IPv6 Snooping VLAN Setup 293
25.16 IPv6 DHCP Trust Setup 294
25.17 Technical Reference 295
25.17.1 DHCP Snooping Overview 295
25.17.2 ARP Inspection Overview 297

Chapter 26
Loop Guard 299

26.1 Loop Guard Overview 299
26.2 Loop Guard Setup 301

Chapter 27
VLAN Mapping 303

27.1 VLAN Mapping Overview 303
27.1.1 VLAN Mapping Example 303
27.2 Enabling VLAN Mapping 303
27.3 Configuring VLAN Mapping 305

Chapter 28
Layer 2 Protocol Tunneling 307

28.1 Layer 2 Protocol Tunneling Overview 307
28.1.1 Layer-2 Protocol Tunneling Mode 308
28.2 Configuring Layer 2 Protocol Tunneling 308

Chapter 29
sFlow 312

29.1 sFlow Overview 312
29.2 sFlow Port Configuration 312
29.2.1 sFlow Collector Configuration 314

Chapter 30
PPPoE 316

30.1 PPPoE Intermediate Agent Overview 316
30.1.1 PPPoE Intermediate Agent Tag Format 316
30.1.2 Sub-Option Format 316
30.1.3 Port State 317
30.2 The PPPoE Screen 318
30.3 PPPoE Intermediate Agent 318
30.3.1 PPPoE IA Per-Port 320
30.3.2 PPPoE IA Per-Port Per-VLAN 322
30.3.3 PPPoE IA for VLAN 323

Chapter 31
Error Disable 325

31.1 Error Disable Overview 325
31.1.1 CPU Protection Overview 325
31.1.2 Error-Disable Recovery Overview 325
31.1.3 What You Can Do 325
31.2 The Error Disable Screen 326
31.3 Error-Disable Status 326
31.4 CPU Protection Configuration 328
31.5 Error-Disable Detect Configuration 330
31.6 Error-Disable Recovery Configuration 331

Chapter 32
MAC Pinning 333

32.1 MAC Pinning Overview 333
32.2 MAC Pinning Configuration 333

Chapter 33
Private VLAN 336

33.1 Private VLAN Overview 336
33.1.1 Configuration 337

Chapter 34
Green Ethernet 340

34.1 Green Ethernet Overview 340
34.2 Configuring Green Ethernet 340

Chapter 35
Link Layer Discovery Protocol (LLDP) 343

35.1 LLDP Overview 343
35.2 LLDP-MED Overview 344
35.3 LLDP Screens 345
35.4 LLDP Local Status 346

35.4.1 LLDP Local Port Status Detail 348
35.5 LLDP Remote Status 352
35.5.1 LLDP Remote Port Status Detail 352
35.6 LLDP Configuration 358
35.6.1 LLDP Configuration Basic TLV Setting 361
35.6.2 LLDP Configuration Basic Org-specific TLV Setting 362
35.7 LLDP-MED Configuration 364
35.8 LLDP-MED Network Policy 366
35.9 LLDP-MED Location 368

Chapter 36
Anti-Arpscan 372

36.1 Anti-Arpscan Overview 372
36.1.1 What You Can Do 372
36.1.2 What You Need to Know 372
36.2 Anti-Arpscan Status 373
36.3 Anti-Arpscan Host Status 374
36.4 Anti-Arpscan Trust Host 374
36.5 Anti-Arpscan Configure 375

Chapter 37
BPDU Guard 378

37.1 BPDU Guard Overview 378
37.1.1 What You Can Do 378
37.2 BPDU Guard Status 378
37.3 BPDU Guard Configuration 379

Chapter 38
OAM 381

38.1 OAM Overview 381
38.1.1 What You Can Do 381
38.2 OAM Status 381
38.2.1 OAM Details 383
38.3 OAM Configuration 387
38.4 OAM Remote Loopback 389

Chapter 39
ZULD 390

39.1 ZULD Overview 390
39.1.1 What You Can Do 390
39.1.2 What You Need to Know 390
39.2 ZULD Status 391
39.3 ZULD Configuration 393

Chapter 40
Static Route 396

40.1 Static Routing Overview 396
40.2 Static Routing 396
40.3 Configuring IPv4 Static Routing 397
40.4 Configuring IPv6 Static Routing 398

Chapter 41
Policy Routing 400

41.1 Policy Route Overview 400
41.1.1 Benefits 400
41.2 Configuring Policy Routing Profile 400
41.2.1 Policy Routing Rule Configuration 401

Chapter 42
Differentiated Services 404

42.1 DiffServ Overview 404
42.1.1 DSCP and Per-Hop Behavior 404
42.1.2 DiffServ Network Example 404
42.2 Two Rate Three Color Marker Traffic Policing 405
42.2.1 TRTCM - Color-blind Mode 406
42.2.2 TRTCM - Color-aware Mode 406
42.3 Activating DiffServ 406
42.3.1 Configuring 2-Rate 3 Color Marker Settings 408
42.3.2 DSCP Profile 410
42.4 DSCP-to-IEEE 802.1p Priority Settings 411
42.4.1 Configuring DSCP Settings 412

Chapter 43
DHCP 413

43.1 DHCP Overview 413
43.1.1 DHCP Modes 413
43.1.2 DHCP Configuration Options 413
43.2 DHCP Configuration 413
43.3 DHCPv4 Status 414
43.3.1 DHCPv4 Server Status Detail 414
43.4 DHCPv4 Relay 415
43.4.1 DHCPv4 Relay Agent Information 416
43.4.2 DHCPv4 Option 82 Profile 416
43.4.3 Configuring DHCPv4 Global Relay 418
43.4.4 DHCPv4 Global Relay Port Configure 418
43.4.5 Global DHCP Relay Configuration Example 420
43.5 Configuring DHCP VLAN Settings 420

43.5.1 DHCPv4 VLAN Port Configure 422
43.5.2 Example: DHCP Relay for Two VLANs 423
43.6 DHCPv6 Status 424
43.7 DHCPv6 Information 425
43.8 DHCPv6 Prefix Delegation 426
43.9 DHCPv6 Relay 428

Chapter 44
VRRP 430

44.1 VRRP Overview 430
44.2 VRRP Status 431
44.3 VRRP Configuration 431
44.3.1 IP Interface Setup 431
44.3.2 VRRP Parameters 433
44.3.3 Configuring VRRP Parameters 433
44.3.4 Viewing VRRP Summary 434
44.4 VRRP Configuration Examples 435
44.4.1 One Subnet Network Example 435
44.4.2 Two Subnets Example 436

Chapter 45
Load Sharing 439

45.1 Load Sharing Overview 439
45.2 Configuring Load Sharing 439

Chapter 46
ARP Setup 441

46.1 ARP Overview 441
46.1.1 How ARP Works 441
46.1.2 ARP Learning Mode 441
46.2 ARP Setup 443
46.2.1 ARP Learning 443
46.2.2 Static ARP 445

Chapter 47
Maintenance 447

47.1 The Maintenance Screen 447
47.2 Firmware Upgrade 448
47.3 Restore a Configuration File 450
47.4 Backup a Configuration File 451
47.5 Erase Running-Configuration 451
47.6 Save Configuration 452
47.7 Reboot System 452

47.7.1 Load Stacking Default 452
47.7.2 Load Factory Default 453
47.8 Tech-Support 453
47.9 FTP Command Line 455
47.9.1 Filename Conventions 455
47.9.2 FTP Command Line Procedure 456
47.9.3 GUI-based FTP Clients 456
47.9.4 FTP Restrictions 457

Chapter 48
Access Control 458

48.1 Access Control Overview 458
48.1.1 What You Can Do 458
48.2 The Access Control Main Screen 458
48.3 About SNMP 459
48.3.1 SNMP v3 and Security 460
48.3.2 Supported MIBs 460
48.3.3 SNMP Traps 461
48.3.4 Configuring SNMP 465
48.3.5 Configuring SNMP Trap Group 466
48.3.6 Enabling/Disabling Sending of SNMP Traps on a Port 467
48.3.7 Configuring SNMP User 469
48.4 Setting Up Login Accounts 471
48.5 SSH Overview 472
48.6 How SSH works 473
48.7 SSH Implementation on the Switch 474
48.7.1 Requirements for Using SSH 474
48.8 Introduction to HTTPS 474
48.9 HTTPS Example 475
48.9.1 Internet Explorer Warning Messages 475
48.9.2 Mozilla Firefox Warning Messages 477
48.9.3 The Main Screen 478
48.10 Service Access Control 479
48.11 Remote Management 480

Chapter 49
Diagnostic 482

49.1 Diagnostic 482

Chapter 50
System Log 485

50.1 Overview 485
50.2 System Log 485

Chapter 51
Syslog Setup 486

51.1 Syslog Overview 486
51.2 Syslog Setup 486

Chapter 52
Cluster Management 489

52.1 Clustering Management Status Overview 489
52.2 Cluster Management Status 490
52.2.1 Cluster Member Switch Management 491
52.3 Clustering Management Configuration 493

Chapter 53
MAC Table 495

53.1 MAC Table Overview 495
53.2 Viewing the MAC Table 496

Chapter 54
IP Table 498

54.1 IP Table Overview 498
54.2 Viewing the IP Table 499

Chapter 55
ARP Table 500

55.1 ARP Table Overview 500
55.1.1 How ARP Works 500
55.2 The ARP Table Screen 500

Chapter 56
Routing Table 502

56.1 Overview 502
56.2 Viewing the Routing Table Status 502

Chapter 57
Path MTU Table 503

57.1 Path MTU Overview 503
57.2 Viewing the Path MTU Table 503

Chapter 58
Configure Clone 504

58.1 Configure Clone 504

Chapter 59
IPv6 Neighbor Table 508

59.1 IPv6 Neighbor Table Overview 508
59.2 Viewing the IPv6 Neighbor Table 508

Chapter 60
Troubleshooting 510

60.1 Power, Hardware Connections, and LEDs 510
60.2 Switch Access and Login 511
60.3 Switch Configuration 513

Appendix A Common Services 514

Appendix B IPv6 517

Appendix C Customer Support 526

Appendix D Legal Information 533

Index 539

PART I
User's Guide

1

Getting to Know Your Switch

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

1.1 Introduction

Your Switch is a layer 2+, Gigabit Ethernet (GbE) switch with two power slots for hot-swappable RPS300 or RPS600-HP power modules. The Switch provides four SFP or SFP+ slots for uplink. By integrating router functions, the Switch performs wire-speed layer-3 routing in addition to layer-2 switching.

This User's Guide covers the following models: GS3700-24, GS3700-24HP, GS3700-48, GS3700-48HP, XGS3700-24, XGS3700-24HP, XGS3700-48, and XGS3700-48HP.

Table 1 Switch Comparison Table

PORT/SWITCH DETAILS	GS3700-24	GS3700-24HP	GS3700-48	GS3700-48HP	XGS3700-24	XGS3700-24HP	XGS3700-48	XGS3700-48HP
24 10/100/1000Base-T Ethernet ports	✓	✓			✓	✓		
48 10/100/1000Base-T Ethernet ports			✓	✓			✓	✓
4 1GbE SFP slots	✓	✓	✓	✓				
4 10GbE SFP+ slots					✓	✓	✓	✓
Supports IEEE 802.3af and IEEE 802.3at PoE standards		✓		✓		✓		✓
Supports IEEE 802.3az EEE Energy Efficient Ethernet (EEE)	✓	✓	✓	✓	✓	✓	✓	✓

With its built-in web configurator, including the ZyXEL One Network (ZON) Neighbor Management feature (Section 5.4 on page 49), viewing, managing and configuring the Switch and its neighboring devices 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.

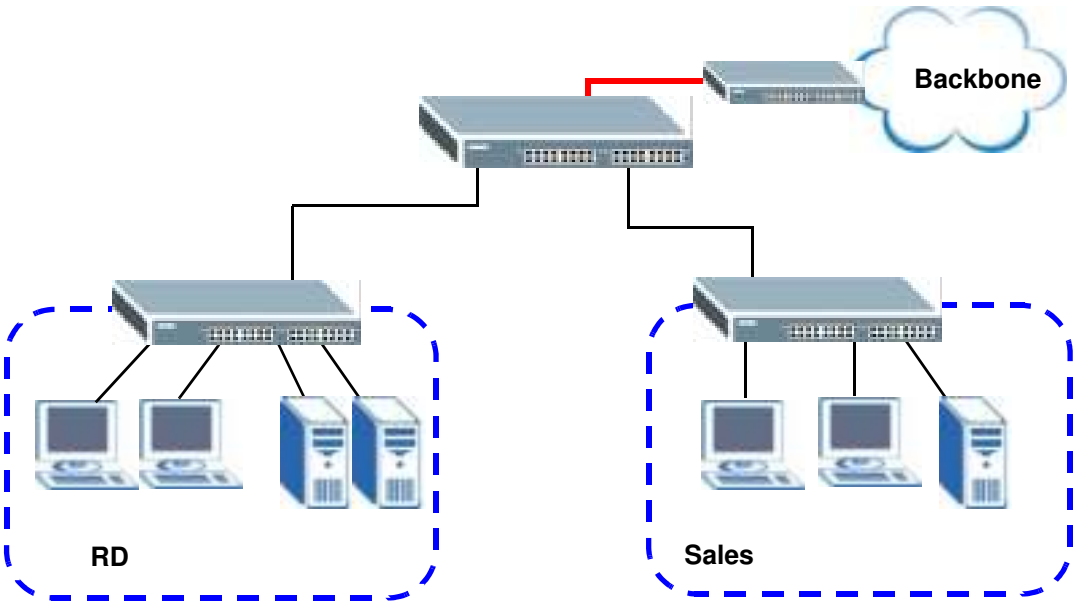
In addition, ZyXEL offers a proprietary software program called ZyXEL One Network (ZON) Utility, it is a utility tool that assists you to set up and maintain network devices in a more simple and efficient way. You can download the ZON Utility at www.zyxel.com and install it on a PC. For more information on ZON Utility see Section 5.3 on page 49.

See the datasheet for a full list of software features available on the Switch.

1.1.1 Bridging Example

In this example the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using the optional 10 Gigabit uplink module on the Switch.

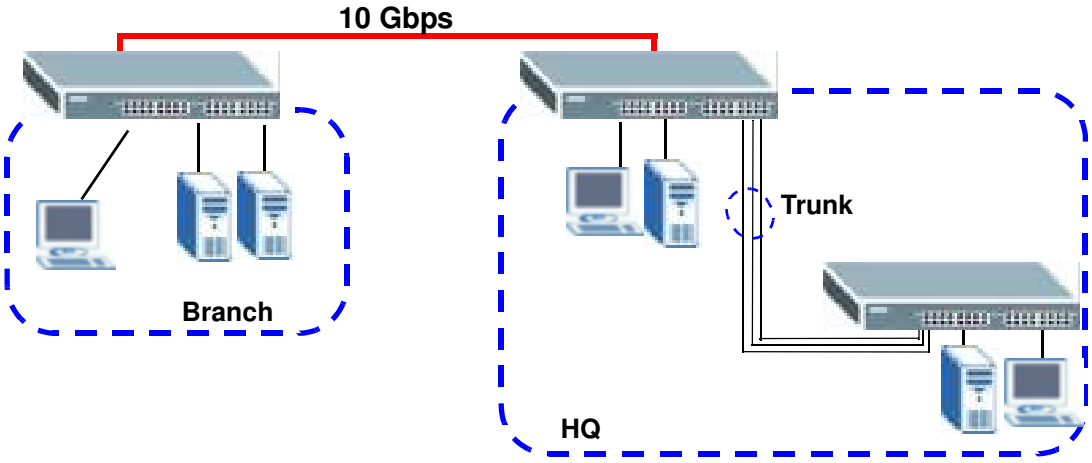
Figure 1 Bridging Application



1.1.2 High Performance Switching Example

The Switch is ideal for connecting two geographically dispersed networks that need high bandwidth. In the following example, a company uses the optional 10 Gigabit uplink modules to connect the headquarters to a branch office network. Within the headquarters network, a company can use trunking to group several physical ports into one logical higher-capacity link. Trunking can be used 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.

Figure 2 High Performance Switching

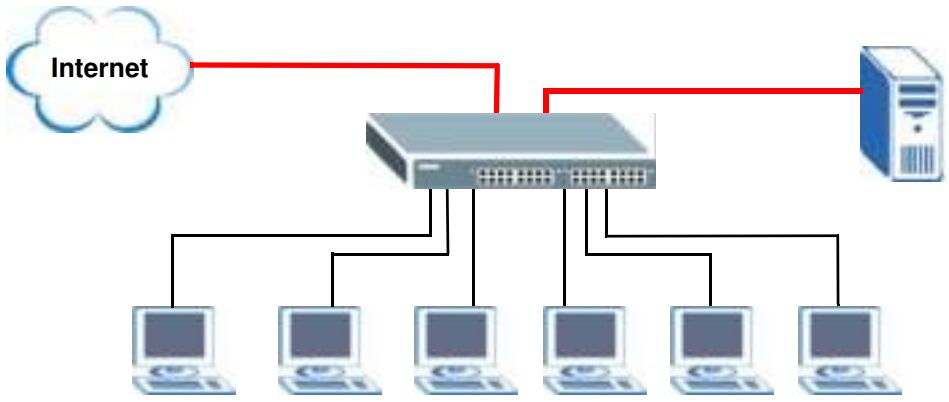


1.1.3 Gigabit Ethernet to the Desktop

The Switch is an ideal solution for small networks which demand high bandwidth for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch. Use the optional 10 Gigabit uplink module to provide high speed access to a data server and the Internet. The uplink module supports a fiber-optic connection which alleviates the distance limitations of copper cabling.

In this example, all computers can share high-speed applications on the server and access the Internet. To expand the network, simply add more networking devices such as switches, routers, computers, print servers and so on.

Figure 3 Gigabit to the Desktop



1.1.4 IEEE 802.1Q VLAN Application Example

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

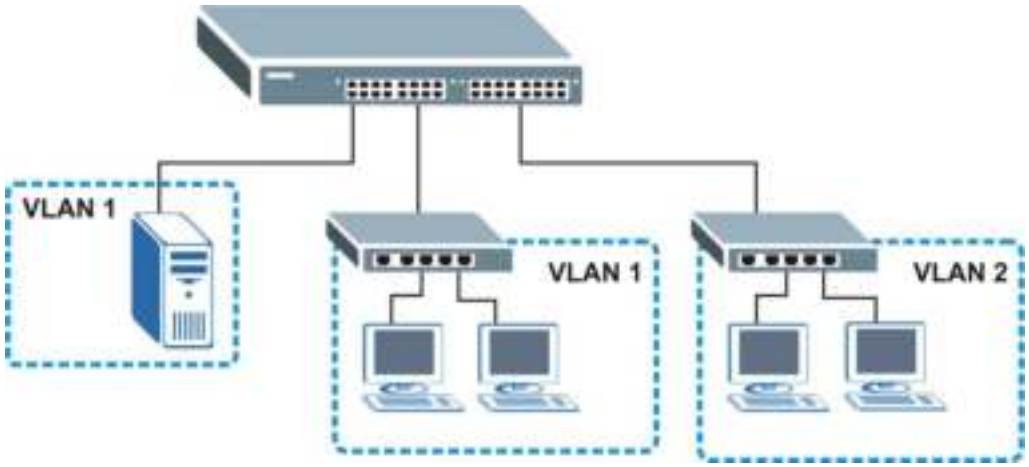
For more information on VLANs, refer to Chapter 7 on page 101.

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain, thus increasing network performance by reducing broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



1.1.5 IPv6 Support

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 x 10^{38} IP addresses. At the time of writing, the Switch supports the following features.

- Static address assignment and stateless auto-configuration
- Neighbor Discovery Protocol (a protocol used to discover other IPv6 devices in a network)
- Remote Management using ping SNMP, telnet, HTTP and FTP services
- ICMPv6 to report errors encountered in packet processing and perform diagnostic functions, such as "ping"
- IPv4/IPv6 dual stack; the Switch can run IPv4 and IPv6 at the same time
- DHCPv6 client and relay
- Multicast Listener Discovery (MLD) snooping and proxy

For more information on IPv6, refer to Appendix B on page 517 and the CLI Reference Guide.

1.2 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 37.
- Command Line Interface. Line commands offer an alternative to the Web Configurator and may be necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See Section 47.9 on page 455.
- SNMP. The device can be monitored and/or managed by an SNMP manager. See Section 48.3 on page 459.

1.3 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.

2

Hardware Installation and Connection

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

2.1 Freestanding Installation

1 Make sure the Switch is clean and dry.

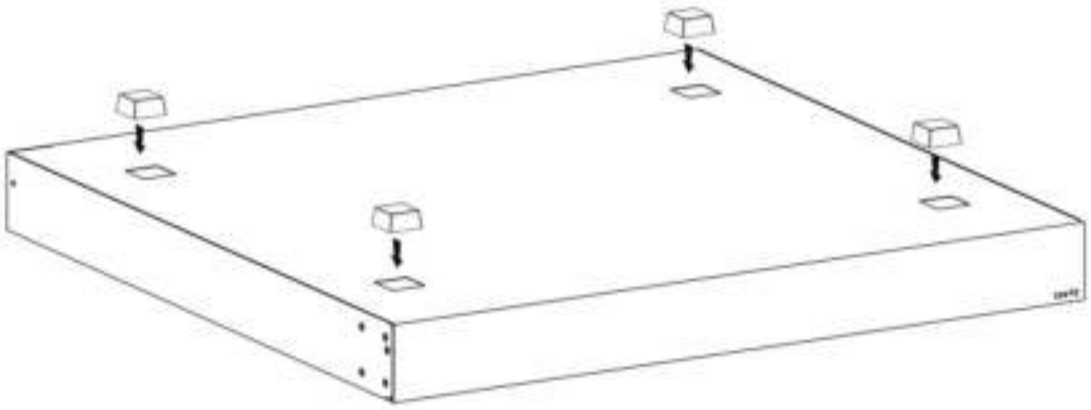
2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.

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 5 Attaching Rubber Feet



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

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. This is especially important for enclosed rack installations.

2.2 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps of how to mount the Switch in a 19-inch rack with the included rack mounting kit.

Note: ZyXEL provides extensible rear mounting brackets (RM400) to install the Switch in a 21-inch, 23-inch or 24-inch rack. See the **RM400 Hardware Installation Guide**.

2.3 Installation Requirements

- Two front mounting brackets (short), two sliding rails and two rear mounting brackets.
- Eight M4 metric screws with large heads and a #2 Philips screwdriver for attaching the brackets to the Switch.
- Four M4 metric screws with small heads and a #2 Philips screwdriver for attaching the sliding rails to the Switch.
- Eight M6 metric rack screws and a screwdriver for attaching the Switch (with attached brackets) to the rack. Rack depth can be from 90 to 120 cm.

Note: Failure to use the proper screws may damage the unit.

2.3.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains. The maximum weight a bracket can hold is 27 Kg.
- 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.

2.4 Attaching the Brackets to the Switch

Use the M4 screws (smaller than the rack screws) to attach the brackets to the Switch.

1 Position the smaller front 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.

2 Use a #2 Philips screwdriver to install the M4 screws with large heads through the mounting bracket holes into the Switch.

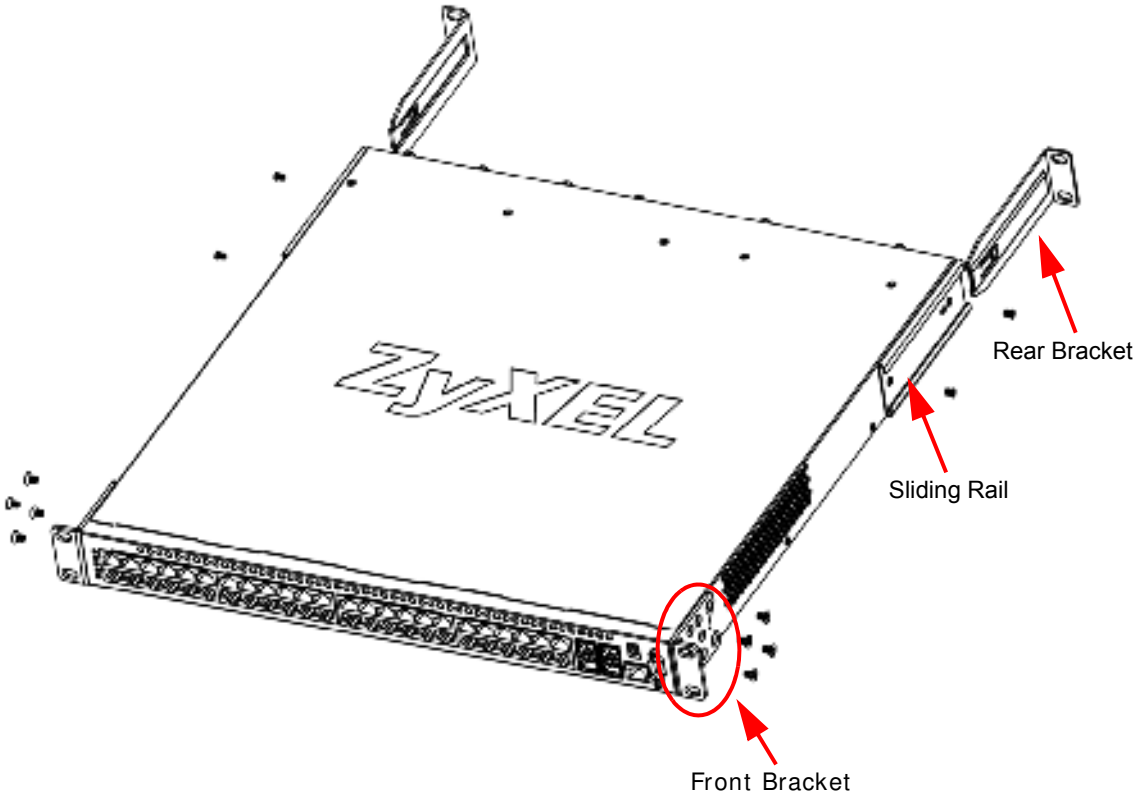
3 Repeat steps 1 and 2 to install the second front mounting bracket on the other side of the Switch.

4 Position a sliding rail on one side at the rear of the Switch, lining up the two screw holes on the sliding rail with the screw holes on the side of the Switch.

5 Use a screwdriver to install the M4 screws with small heads through the sliding rail holes into the Switch.

6 Repeat steps 1 and 2 to install the second sliding rail on the other side of the Switch.

7 Slide the rear bracket along the rail and set the bracket in place depending on the depth of the rack. The rear brackets can be used with a 19-inch rack.



You may now mount the Switch on a rack. Proceed to the next section.

2.5 Mounting the Switch on a Rack

Use the M6 rack screws (larger than the M4 screws) to mount the Switch with brackets on the rack.

1 Position a front 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 at the front of the rack.

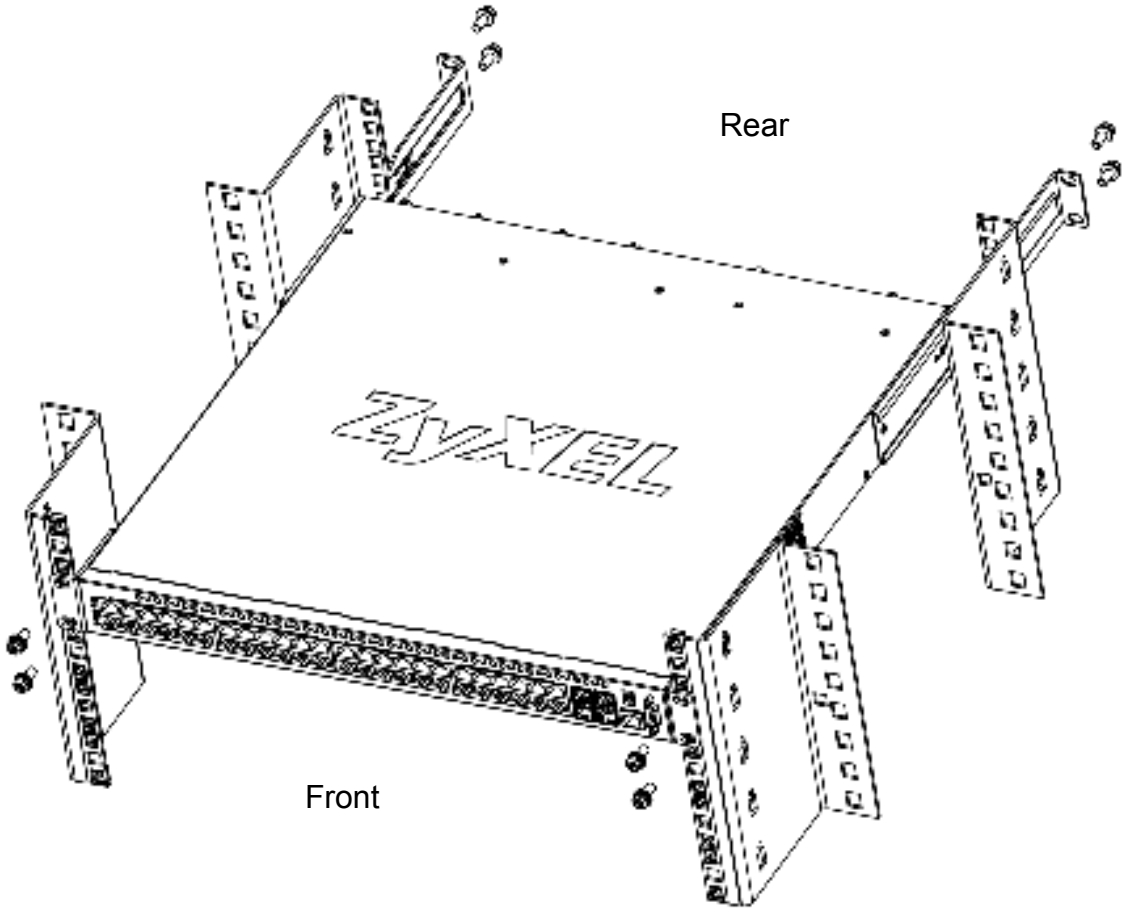
2 Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the other front mounting bracket on the other side of the rack.

4 Position a rear 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 at the rear of the rack.

5 Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.

6 Repeat steps 4 and 5 to attach the other rear mounting bracket on the other side of the rack.



2.6 Power Module Installation

There is one power module installed in the first power slot of the Switch by default. See the **Power Module Hardware Installation Guide** for how to install a second power module or remove the power module.

3

Hardware Overview

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

3.1 Front Panel Connections

The figure below shows the front panel of the Switch.

Figure 6 Front Panel: GS3700 Series

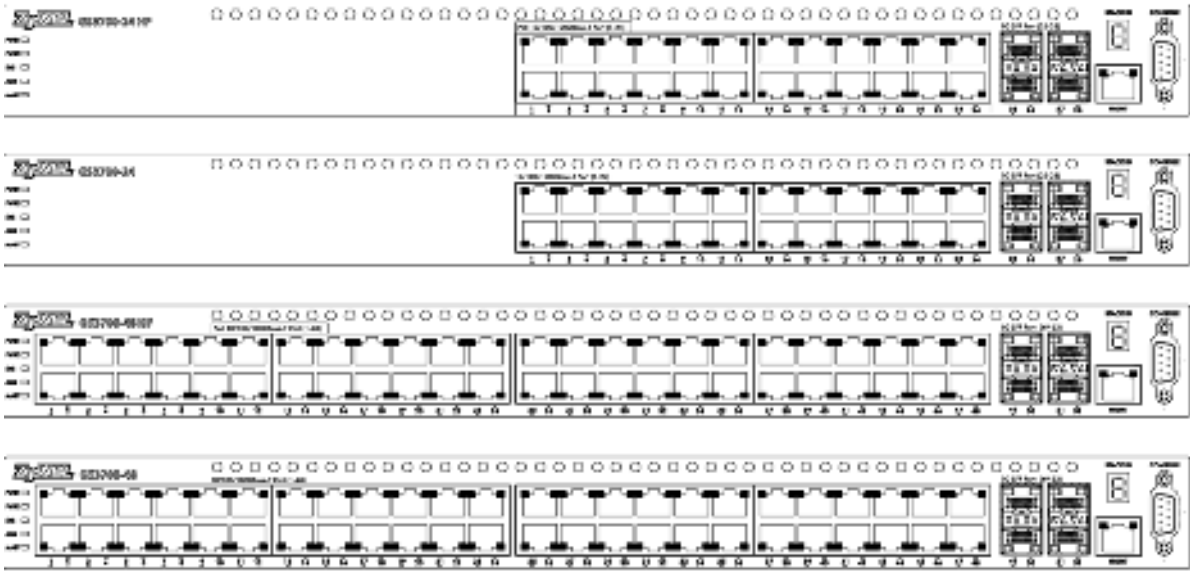
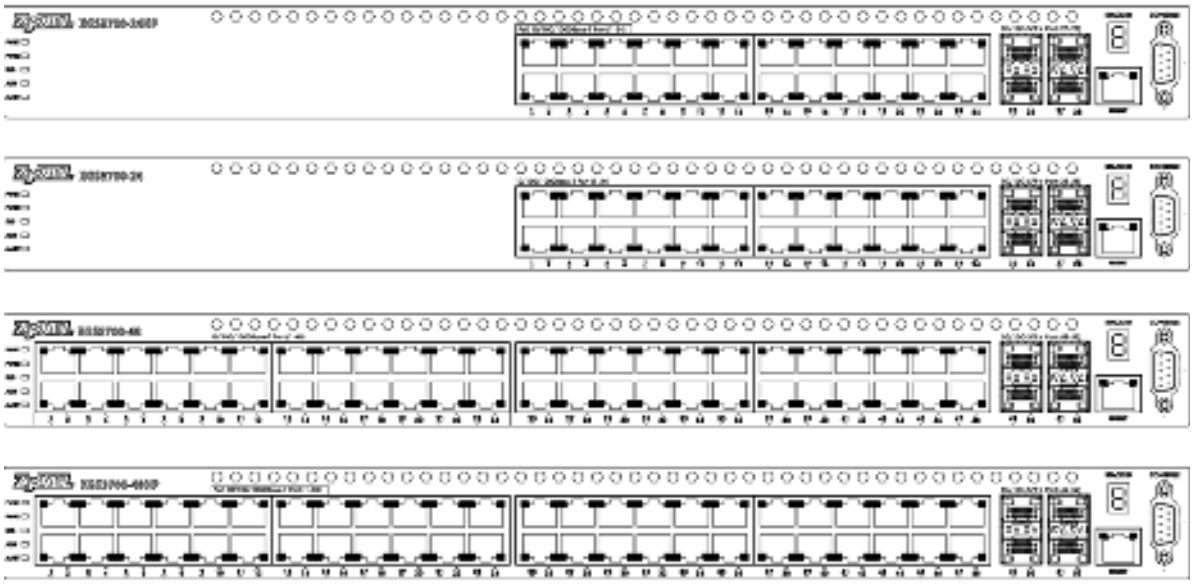


Figure 7 Front Panel: XGS3700 Series



The following table describes the ports.

Table 2 Panel Connections

CONNECTOR	DESCRIPTION
24 or 48 10/100/1000Base-T RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
4 SFP or SFP+ Slots	Use Small Form-Factor Pluggable (SFP) or SFP+ transceivers in these ports for fiber-optic or copper connections to a computer, a hub, an Ethernet switch or router. You can also insert an SFP+ Direct Attach Copper (DAC) in the SFP+ slot.
RJ-45 out-of-band Management Port	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the Switch.
Console Port	Only connect this port to your computer (using an RS-232 cable) if you want to configure the Switch using the command line interface (CLI) via the console port.

3.1.1 Ethernet Ports

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

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.

3.1.1.1 Default Ethernet Settings

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

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Dual Personality Interface: Fiber-optic module first

3.1.2 SFP/SFP+ Slots

These are four slots for Small Form-Factor Pluggable (SFP) or SFP+ modules, such as an SFP/SFP+ transceiver. The SFP+ (SFP Plus) is an enhanced version of the SFP and supports data rates of 10 Gbps. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the Switch. 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 connectors.

- Type: SFP or SFP+ connection interface
- Connection speed: 1 or 10 Gigabit per second (Gbps)

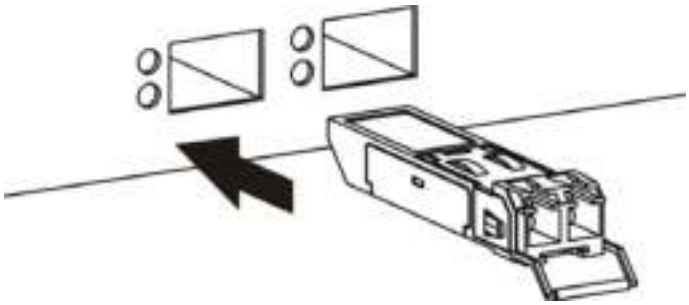
To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.2.1 Transceiver Installation

Use the following steps to install a transceiver.

1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

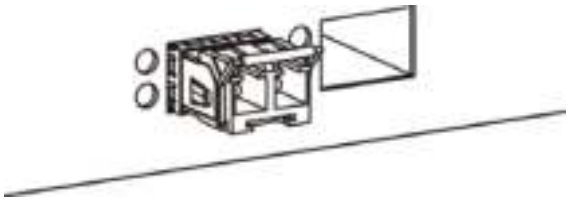
Figure 8 Transceiver Installation Example



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.

Figure 9 Installed Transceiver



3.1.2.2 Transceiver Removal

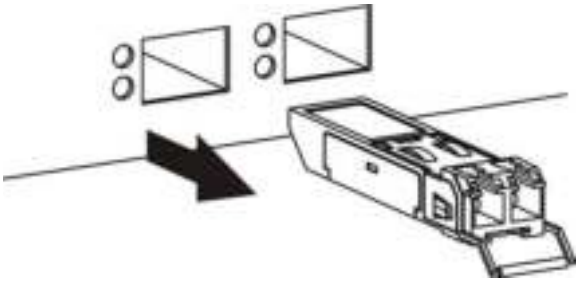
Use the following steps to remove a transceiver.

1 Open the transceiver's latch (latch styles vary).

Figure 10 Opening the Transceiver's Latch Example

2 Pull the transceiver out of the slot.

Figure 11 Transceiver Removal Example



3.1.3 Management Port

The 100Base-T Ethernet **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.

3.1.4 Console Port

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

- VT100 terminal emulation
- 9600 bps

- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the RS-232 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.

3.2 Rear Panel

The following figures show the rear panels of the Switch. The rear panels contain:

- A slot for a fan module (**A**)
- Two slots for power modules with power receptacles (**B** and **C**)

Figure 12 Rear Panel

3.2.1 Removing and Installing the Fan Module

See the **Fan Module Hardware Installation Guide** to see how to install the fan module in the Switch.

3.2.2 Power Connection

Make sure you are using the correct power source and that no objects obstruct the airflow of the fans.

The Switch uses two power supply modules, one of which is redundant, so if one power module fails the system can operate on the remaining module.

Connecting the Power

Use the following procedures to connect the Switch to a power source after you have installed it in a rack.

Note: Use the included power cord for the AC power connection.

1 Connect the female end of the power cord to the AC power socket.

2 Connect the other end of the cord to a power outlet.

Disconnecting the Power

The power input connectors can be disconnected from the power source individually.

1 Disconnect the power cord from the power outlet.

2 Disconnect the power cord from the AC power socket.

3.3 LEDs

The following table describes the LEDs.

Table 3 LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR1 (Power 1)	Green	On	The system is receiving power from the power module in the first power slot.
		Off	The system is not receiving power from the power module in the first power slot.
	Amber	On	The power module in the first power slot fails to supply power or its fan is not functioning at a proper speed.
PWR2 (Power 2)	Green	On	The system is receiving power from the power module in the second power slot.
		Off	The system is not receiving power from the power module in the second power slot.
	Amber	On	The power module in the second power slot fails to supply power or its fan is not functioning at a proper speed.
SYS (System)	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready or malfunctioning.
ALM (Alarm)	Red	On	There is a hardware failure, such as high device temperature, wrong voltage and abnormal fan speed.
		Off	The system is functioning normally.
MAST (Master)	Green	On	The Switch is acting as a standalone switch or the master in stacking.
		Off	The Switch is acting as a non-master member in a stack or it is in standalone mode.
10/100/1000Base-T Ports			
1-24 or 1-48 LNK/ACT (Left)	Green	Blinking	The port is receiving or transmitting data at 10 or 1000 Mbps.
		On	The port has a successful 10 or 1000 Mbps connection.
	Amber	Blinking	The port is receiving or transmitting data 100 Mbps.
		On	The port has a successful 100 Mbps connection.
		Off	This link is disconnected or the port is disabled.
PoE 10/100/1000Base-T Ports			
1-24 or 1-48 LNK/ACT (Left)	Green	Blinking	The port is receiving or transmitting data at 10 or 1000 Mbps.
		On	The port has a successful 10 or 1000 Mbps connection.
	Amber	Blinking	The port is receiving or transmitting data 100 Mbps.
		On	The port has a successful 100 Mbps connection.
		Off	This link is disconnected or the port is disabled.

Table 3 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
1-24 or 1-48 POE (Right)	Green	On	Power is supplied to the PoE port.
		Off	Power is not supplied to the PoE port.
1G SFP Slots			
25-28 or 49-52 LNK/ACT	Green (Right)	Blinking	The port is receiving or transmitting data at 1 Gbps.
		On	The port has a successful 1 Gbps connection.
		Off	This link is disconnected.
1G/10G SFP+ Slots			
25-28 or 49-52 LNK/ACT	Green (Right)	Blinking	The port is receiving or transmitting data at 1 Gbps.
		On	The port has a successful 1 Gbps connection.
	Blue (Left)	Blinking	The port is receiving or transmitting data 10 Gbps.
		On	The port has a successful 10 Gbps connection.
		Off	This link is disconnected.
STACK ID			The LED is showing the Stack ID number of the Switch. ID 0 means it is a standalone Switch.
MGMT (Management)	Green	Blinking	The system is transmitting or receiving to/from an Ethernet device at 10 Mbps through the **MGMT** port.
		On	The **MGMT** port is connected at 10 Mbps.
		Off	The **MGMT** port is not connected at 10 Mbps, to an Ethernet device, or the port is disabled.
	Amber	Blinking	The system is transmitting or receiving to/from an Ethernet device at 100 Mbps through the **MGMT** port.
		On	The **MGMT** port is connected at 100 Mbps.
		Off	The **MGMT** port is not connected at 100 Mbps, to an Ethernet device, or the port is disabled.

4

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. Supported browsers at the time of writing are:

- IE 8 or later
- Chrome 34.0.1847.131 or later
- Firefox 29.0.1 or later
- Opera 21.0 or later
- Safari 5.1.7 or later

The recommended screen resolution is 1024 by 768 pixels. 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 some browsers.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

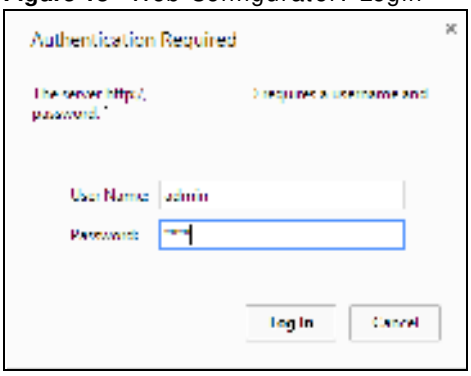
4.2 System Login

1 Start your web browser.

2 Type “http://” and the IP address of the Switch (for example, the default management IP address is 192.168.1.1 through an in-band (non-**MGMT**) port and 192.168.0.1 through the **MGMT** port) in the Location or Address field. Press [ENTER]. Your computer must be in the same subnet in order to access this website address.

3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 13 Web Configurator: Login



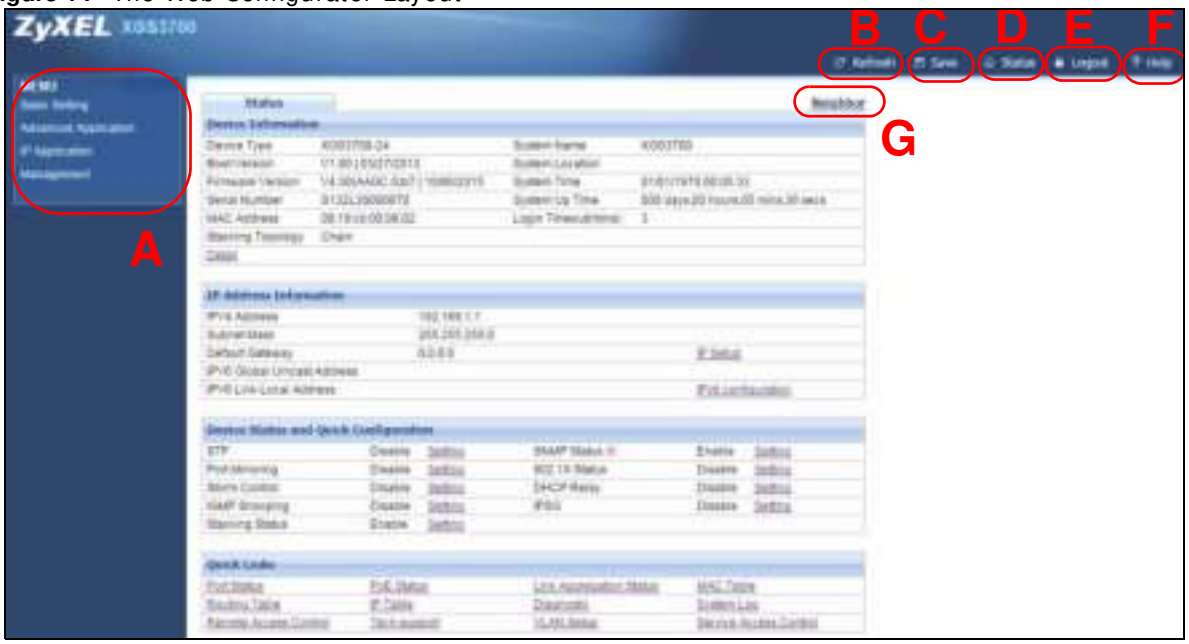
4 Click **OK** to view the first web configurator screen.

4.3 The Web Configurator Layout

The **Status** screen is the first screen that displays when you access the web configurator. This guide uses the XGS3700-48HP screens as an example. The screens may vary slightly for different models.

The following figure shows the navigating components of a web configurator screen.

Figure 14 The Web Configurator Layout



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**, **F**- 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 update the information in the screen you are viewing currently.

C - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is saved in the configuration file from which the Switch booted from and it stays the same even if the Switch's power is turned off. See Section 47.6 on page 452 for information on saving your settings to a specific configuration file.

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

E - Click this link to log out of the web configurator.

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

G - Click this link to go to the ZON **Neighbor** Management screen where you can see and manage neighbor devices learned by the Switch.

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

Table 4 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
MENU Basic Setting Advanced Application IP Application Management System Info General Setup Switch Setup IP Setup Port Setup PoE Setup Interface Setup IPv6 Stacking DNS	MENU Basic Setting Advanced Application IP Application Management VLAN Static MAC Forwarding Static Multicast Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Authentication Port Security Time Range Classifier Policy Rule Queuing Method VLAN Stacking Multicast AAA IP Source Guard Loop Guard VLAN Mapping Layer 2 Protocol Tunneling sFlow PPPoE Errdisable MAC Pinning Private VLAN Green Ethernet LLDP Anti-Arpscan BPDU Guard OAM ZULD	MENU Basic Setting Advanced Application IP Application Management Static Routing Policy Routing DiffServ DHCP VRRP Load Sharing ARP Setup	MENU Basic Setting Advanced Application IP Application Management Maintenance Access Control Diagnostic System Log Syslog Setup Cluster Management MAC Table IP Table ARP Table Routing Table Path MTU Table Configure Clone IPv6 Neighbor Table Port Status

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 and time settings for 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 IP address, subnet mask (necessary for Switch management) and set up to 128 IP routing domains.
Port Setup	This link takes you to screens where you can configure speed, flow control and priority settings for individual Switch ports.
PoE Setup	For PoE model(s). This link takes you to a screen where you can set priorities, PoE power-up settings and schedule so that the Switch is able to reserve and allocate power to certain PDs.
Interface Setup	This link takes you to a screen where you can create IPv6 interfaces on the Switch.
IPv6	This link takes you to a screen where you can enable an IPv6 interface and configure the IPv6 settings on the Switch.
Stacking	This link takes you to a screen where you can view and configure stacking system for the Switch.
DNS	This link takes you to a screen where you can configure DNS (domain name server) IP addresses.
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 Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to screens 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.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed on a port.
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 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.
Port Security	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.
Time Range	This link takes you to a screen where you can configure time range for time-oriented features like Classifier.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Classifier	This link takes you to screens 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 screens where you can activate and configure VLAN stacking.
Multicast	This link takes you to screen where you can configure various multicast features, IGMP snooping, MLD snooping-proxy and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication, authorization and accounting services 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.
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.
sFlow	This link takes you to screens where you can configure sFlow settings on the Switch.
PPPoE	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.
Errdisable	This link takes you to a screens where you can view errdisable status and configure errdisable settings in CPU protection, errdisable detect, and errdisable recovery.
MAC Pinning	This link takes you to a screen where you can set specific ports to have priority over other ports in MAC address learning.
Private VLAN	This link takes you to a screen where you can block traffic between ports in a VLAN on the Switch.
Green Ethernet	This link takes you to a screen where you can configure the Switch to reduce port power consumption.
LLDP	This link takes you to a screen where you can configure LLDP settings.
Anti-Arpscan	This link takes you to screens where you can enable anti-arpscan on the Switch and ports, and view the port state. You can also create trusted hosts, view blocked hosts and unblock them.
BPDU Guard	This link takes you to screens where you can enable BPDU guard on the Switch and ports, and view the port state.
OAM	This link takes you to screens where you can enable Ethernet OAM on the Switch, view the configuration of ports on which Ethernet OAM is enabled and perform remote-loopback tests.
ZULD	This link takes you to screens where you can enable ZULD on a port and configure related settigns.
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.
Policy Routing	This link takes you to screens where you can configure policy routing rules.

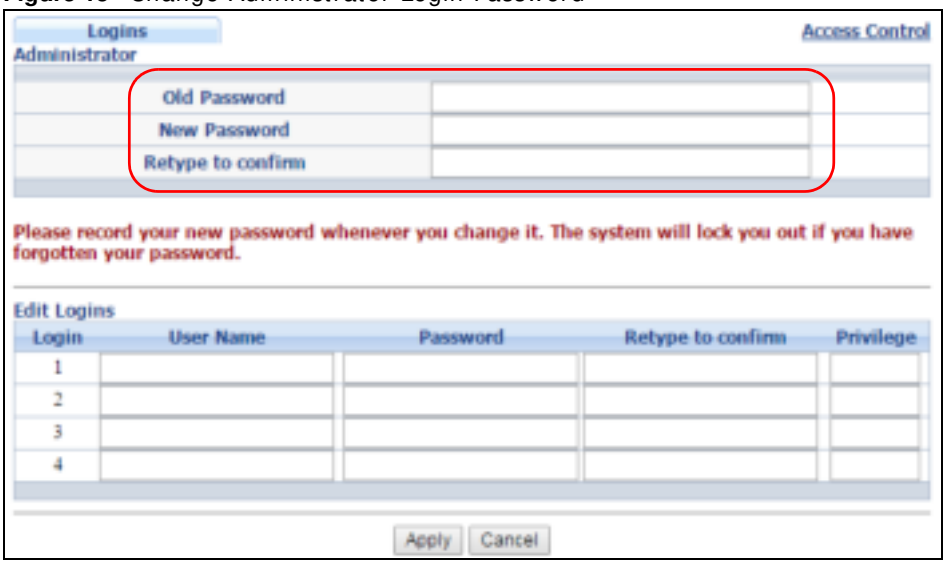
Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
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.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
Load Sharing	This link takes you to a screen where you can enable Equal-Cost MultiPath (ECMP) routing and set the criteria the Switch uses to determine the routing path for a packet.
ARP Setup	This link takes you to a screen where you can configure ARP learning mode on a per-port basis and create static ARP entries which do not age out.
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 screens where you can ping IP addresses, run traceroute, test port(s).
System Log	This link takes you to a screen where you can view system logs.
Syslog Setup	This link takes you to a screen where you can setup system logs and a system log server.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of MAC address it is.
IP Table	This link takes you to a screen where you can view the IP addresses and VLAN ID of a device attached to a port.You can also view what kind of device it is.
ARP Table	This link takes you to a screen where you can view the MAC address – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table.
Path MTU Table	This link takes you to a screen where you can view the IPv6 path MTU table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to (an)other port(s).
IPv6 Neighbor Table	This link takes you to a screen where you can view the Switch's IPv6 neighbor table.
Port Status	This link takes you to a screen where you can view the port statistics.

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 15 Change Administrator Login Password



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 9600bps with 8 data bit, 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. See Section 3.2 on page 34 for details.

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 16 Resetting the Switch: Via the Console Port

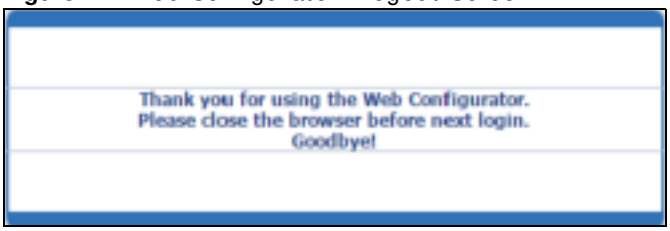
```
Bootbase Version: V1.00 | 12/11/2012 13:49:40
RAM: Size = 524288 Kbytes
DRAM POST: Testing: 524288K
OK
DRAM Test SUCCESS !

ZyNOS Version: V4.10(AAGF.5)b1 | 6/5/2014 20:10:8

Press any key to enter debug mode within 3 seconds.
.................................
Enter Debug Mode
ras> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCC
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 17 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.

PART II
Technical Reference

5

ZON Utility, ZON Neighbor Management and Port Status

5.1 Overview

This chapter describes the screens for System Status, ZON Utility, ZON Neighbor Management, Port Status and Port Details.

5.2 Status

The **Status** screen displays when you log into the Switch or click **Status** at the top right corner of the web configurator. The **Status** screen displays general device information, system status, and its IP addresses.

Figure 18 Status

The following table describes the fields in the above screen.

Table 6 Status

LABEL	DESCRIPTION
Device Information	
Device Type	This field displays the model name of this Switch.
System Name	This field displays the name used to identify the Switch on any network.
Boot Version	This field displays the version number and date of the boot module that is currently on the Switch.
System Location	This field displays the geographic location of your Switch. You can change the setting in the **Basic Setting > General** Setup screen.
Firmware Version	This field displays the version number and date of the firmware the Switch is currently running.
System Time	This field displays the current date and time in the UAG. The format is mm-dd-yyyy hh:mm:ss.
Serial Number	This field displays the serial number of this Switch. The serial number is used for device tracking and control.
System Up Time	This field displays how long the Switch has been running since it last restarted or was turned on.
MAC Address	This field displays the MAC addresses of the Switch.
Login Timeout	This field displays how many minutes a management session can be left idle before the session times out. After it times out you have to log in with your password again.
Stacking topology (Stacking mode)	This field displays whether the current topology is **Chain** or **Ring**.
Detail	Click this link to go to the **Basic Setting > System Info** screen to check other detailed information, such as system resource usage and the Switch temperature, fan speeds or voltage.
IP Address Information	
IPv4 Address	This field displays the Switch's current IPv4 address.
Subnet Mask	This field displays the Switch's subnet mask.
Default Gateway	This field displays the IP address of the Switch's default gateway.
IP Setup	Click the link to go to the **Basic Setting > IP Setup** screen.
IPV6 Global Unicast Address	This field displays the Switch's IPv6 global unicast address.
IPV6 Link-Local Address	This field displays the Switch's IPv6 link-local address.
IPv6 configuration	Click the link to go to the **Basic Setting > IPv6** screen.
Device Status and Quick Configuration	This section shows whether a feature is enabled or not on the Switch. You can click a feature's **Setting** link to go to the configuration screen for the feature. Hover your cursor over a red exclamation mark to display information about the feature. Note: The **Stacking Status** field is displayed only on the Switch with stacking support.
Quick Links	This section provides the shortcut link to a specific cofiguration screen.

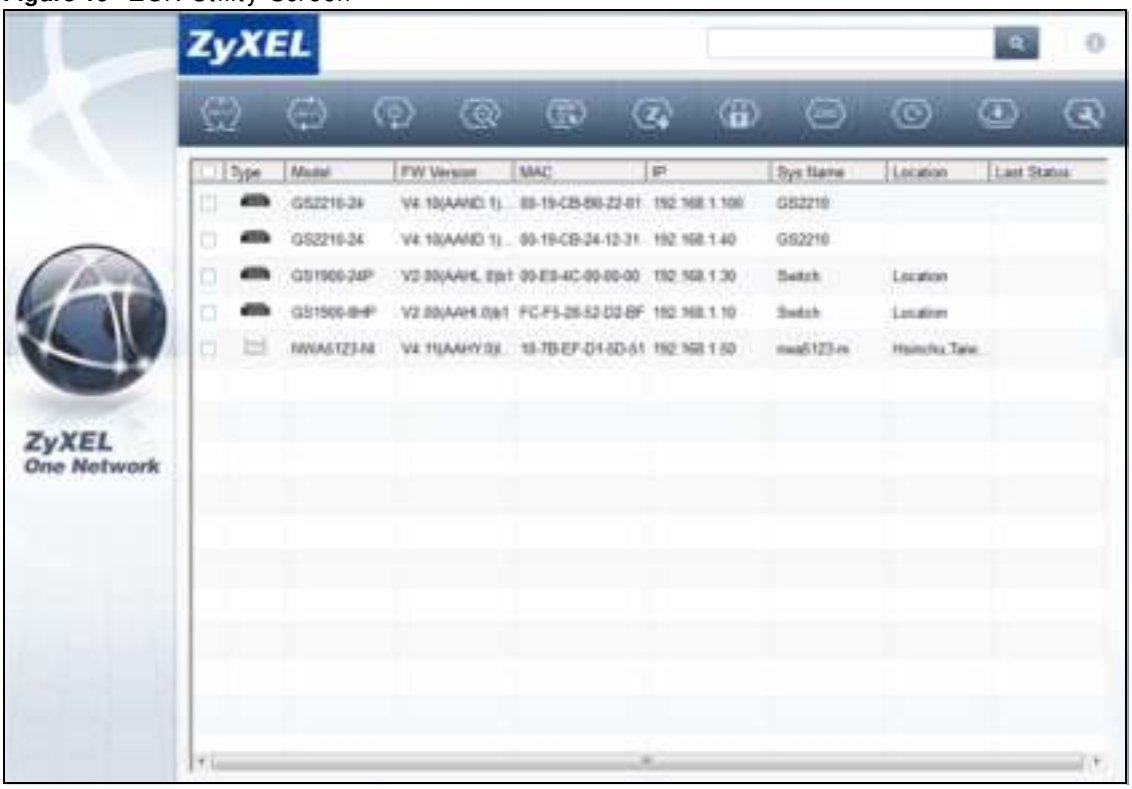
5.3 ZyXEL One Network (ZON) Utility Screen

ZON Utility is a program designed to help you deploy and manage a network more efficiently. It detects devices automatically and allows you to do basic settings on devices in the network without having to be near it.

The ZON Utility issues requests via ZyXEL Discovery Protocol (ZDP) and in response to the query, the device responds back with basic information including IP address, firmware version, location, system and model name in the same broadcast domain. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a PC.

The following figure shows the ZON Utility screen.

Figure 19 ZON Utility Screen



5.4 ZON Neighbor Management Screen

The ZON Neighbor Management screen allows you to view and manage the Switch's neighboring devices more conveniently. It uses Layer Link Discovery Protocol (LLDP) to discover all neighbor devices connected to the Switch including non-ZyXEL devices. You can perform tasks on the neighboring devices like login, reboot (turn the power off and then back on again), and reset to factory default settings in the Neighbor Management screen. For more information on LLDP, see Section 35.2 on page 344.

Click **Status** > **Neighbor** to see the following screen.

Figure 20 Status > Neighbor

The following table describes the fields in the above screen.

Table 7 Status > Neighbor

LABEL	DESCRIPTION
Local	
Port	This shows the port of the Switch, on which the neighboring device is discovered.
Desc.	This shows the port description of the Switch.
PoE Draw	This shows the consumption that the neighboring device connected to this port draws from the Switch. This allows you to plan and use within the power budget of the Switch.
Remote	
Port	This show the number of the neighbor device's port which is connected to the Switch.
Desc.	This shows the description of the neighbor device's port which is connected to the Switch.
Model	This shows the model name of the neighbor device. This field will show "**-**" for non-ZyXEL devices.
System Name	This shows the system name of the neighbor device.
Location	This shows the geographic location of the neighbor device.
Firmware	This shows the firmware version of the neighbor device. This field will show "**-**" for non-ZyXEL devices.
IP	This shows the IP address of the neighbor device. The IP address is a **hyper link** that you can click to log into and manage the neighbor device through its web configurator. This field will show "**-**" for non-ZyXEL devices.
MAC	This shows the MAC address of the neighbor device. This field will show "**-**" for non-ZyXEL devices.
PWR Cycle	Click the **Cycle** button to turn OFF the power of the neighbor device and turn it back ON again. A count down button (from 5 to 0) starts. Note: The Switch must support power sourcing (PSE) or the network device is a powered device (PD). Note: If multiple neighbor devices use the same port, the **Cycle** button is displayed only on the first device, others will show "**-**" instead.
Reset to Default	Click the **Reset** button to reset the neighbor device to its factory default settings. A warning message "**Are you sure you want to load factory default?**" appears prompting you to confirm the action. After confirming the action a count down button (from 5 to 0) starts. Note: The Switch must support power sourcing (PSE) or the network device is a powered device (PD). Note: If multiple neighbor devices use the same port, the **Reset** button is not available and will show "**-**" instead. Note: You can only reset ZyXEL products.

5.5 Port Status

This screen displays a port statistical summary with links to each port showing statistical details. To view the port statistics, click **Status** in all web configurator screens and then the **Port Status** link in the **Quick Links** section of the **Status** screen to display the **Port Status** screen as shown next. You can also click **Management > Port Status** to see the following screen.

Figure 21 Port Status (Standalone mode)

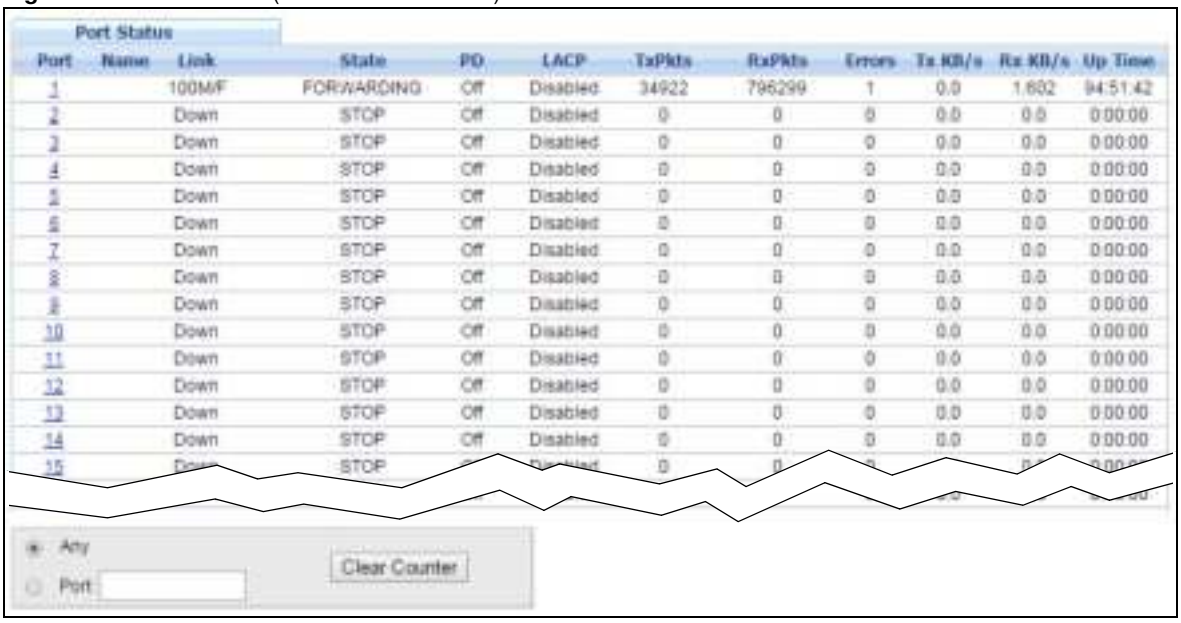
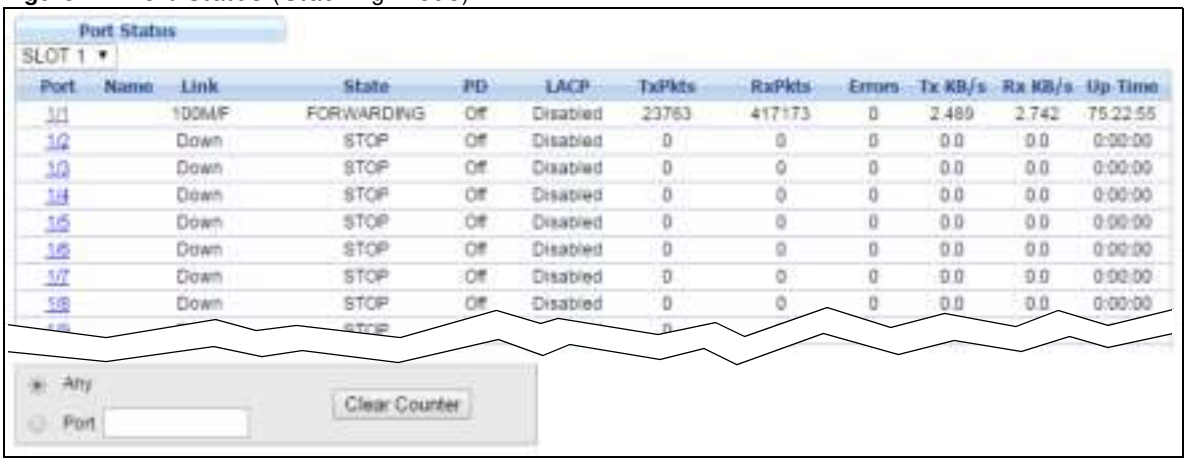


Figure 22 Port Status (Stacking mode)



The following table describes the labels in this screen.

Table 8 Port Status

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This identifies the Ethernet port. In stacking mode, the first number represents the slot and the second the port number. Click a port number to display the **Port Details** screen (refer to Figure 23 on page 53).

Table 8 Port Status

LABEL	DESCRIPTION
Name	This is the name you assigned to this port in the **Basic Setting** > **Port Setup** screen.
Link	This field displays the speed (such as **100M** for 100 Mbps, **1000M** for 1000 Mbps, or **10G** for 10 Gbps) and the duplex (**F** for full duplex). This field displays **Down** if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. (See Section 11.1.3 on page 133 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
PD	(For PoE models only) This field displays whether or not a powered device (PD) is allowed to receive power from the Switch on this port.
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 transmission speed of data sent on this port in kilobytes per second.
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Select **Port**, type a port number and then click **Clear Counter** to erase the recorded statistical information for that port, or select **Any** to clear statistics for all ports.

5.5.1 Port Details

Click a number in the **Port** column in the **Port Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 23 Port Status: Port Details

Port Details		Port Status
Port Info	Port NO.	1
	Name	
	Link	100M/F
	State	FORWARDING
	LACP	Disabled
	TxPkts	35034
	RxPkts	797796
	Errors	1
	Tx KBs/s	0.0
	Rx KBs/s	1.560
	Up Time	94:57:58
TX Packet	Unicast	23640
	Multicast	11394
	Broadcast	0
	Pause	0
	Tagged	0
RX Packet	Unicast	224664
	Multicast	363040
	Broadcast	210091
	Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	1
	Length	0
	Runt	0
Distribution	64	494597
	65 to 127	258969
	128 to 255	54799
	256 to 511	12436
	512 to 1023	4212
	1024 to 1518	7817
	Giant	0

The following table describes the labels in this screen.

Table 9 Port Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing. In stacking mode, the first number represents the slot and the second the port number.
Name	This field displays the name of the port.
Link	This field displays the speed (such as **100M** for 100Mbps, **1000M** for 1000 Mbps, or **10G** for 10 Gbps) and the duplex (**F** for full duplex).
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1.3 on page 133 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
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

Table 9 Port Status: Port Details (continued)

LABEL	DESCRIPTION
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 KBs/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Rx KBs/s	This field shows the transmission speed of data received on this port in kilobytes per second.
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.	
Unicast	This field shows the number of good unicast packets 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.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets 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.
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.
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).
Length	This field shows the number of packets received with a length that was out of range.
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.

Table 9 Port Status: Port Details (continued)

LABEL	DESCRIPTION
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	This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your Switch model.

6

Basic Setting

This chapter describes how to configure the **Basic Setting** screens.

6.1 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.

Figure 24 Basic Setting > System Info (Standalone Mode)

System Info

System Name	XGS3700
Product Model	XGS3700-48HP
ZyNOS F/W Version	V4.30(AAGF.0)b3 | 07/17/2015
Ethernet Address	00:19:cb:00:00:02

CPU Utilization

Current (%)	21.88

Memory Utilization

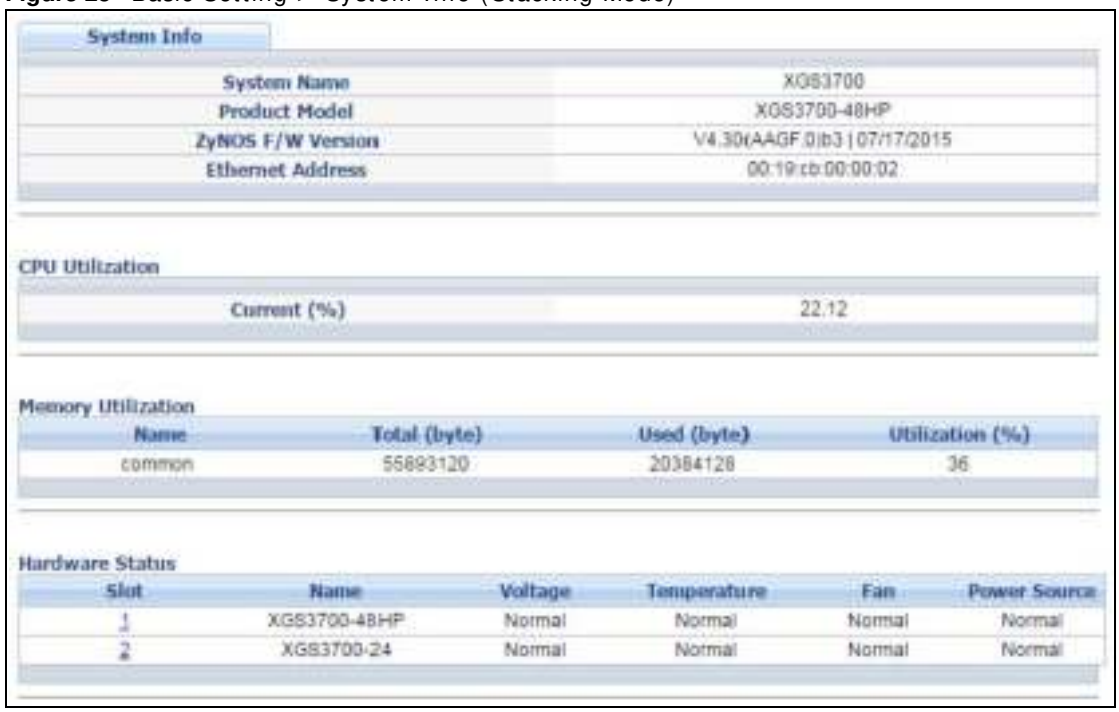
Name	Total (byte)	Used (byte)	Utilization (%)
common	55693120	11315200	20

Hardware Monitor

Temperature Unit: C

Temperature (C)	Current	MAX	MIN	Threshold	Status
MAC	45.0	51.0	44.0	85.0	Normal
CPU	50.0	52.0	45.0	85.0	Normal
PHY_1	46.0	50.0	43.0	85.0	Normal
PHY_2	46.0	50.0	43.0	85.0	Normal
Board_1	44.0	46.0	41.0	85.0	Normal
Board_2	36.0	40.0	34.0	85.0	Normal
FAN Speed (RPM)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
FAN1	4691	9729	4647	500	Normal
FAN2	4761	9623	4728	500	Normal
FAN3	4821	9677	4770	500	Normal
Voltage (V)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
2.5V	2.493	2.493	2.493	+/-6%	Normal
1.8V	1.787	1.787	1.775	+/-6%	Normal
3.3V	3.308	3.308	3.308	+/-6%	Normal
5V	4.988	4.988	4.988	+/-6%	Normal
12V	11.781	11.781	11.781	+/-10%	Normal
1.0V	0.996	0.996	0.983	+/-6%	Normal
0.9V	0.896	0.896	0.896	+/-6%	Normal
3.3V	3.308	3.308	3.308	+/-6%	Normal
1.05V	1.029	1.054	1.029	+/-6%	Normal
1.2V	1.156	1.156	1.156	+/-6%	Normal
Power Source					**Status**
PSU_1					Normal
PSU_2					Absent

Figure 25 Basic Setting > System Info (Stacking Mode)



The following table describes the labels in these screens.

Table 10 Basic Setting > System Info (Standalone and Stacking Modes)

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
Product Model	This field displays the product model of the Switch. Use this information when searching for firmware upgrade or looking for other support information in the website.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
CPU Utilization	CPU utilization quantifies how busy the system is. **Current (%)** displays the current percentage of CPU utilization.
Memory Utilization	Memory Utilization shows how much DRAM memory is available and in use. It also displays the current percentage of memory utilization.
Name	This field displays the name of memory pool.
Total	This field displays the total number of bytes in this memory pool.
Used	This field displays the number of bytes being used in this memory pool.
Utilization	This field displays the percentage (%) of memory being used in this memory pool.
Hardware Monitor (Standalone Mode)	
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	**BOARD**, **MAC** and **PHY** 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.

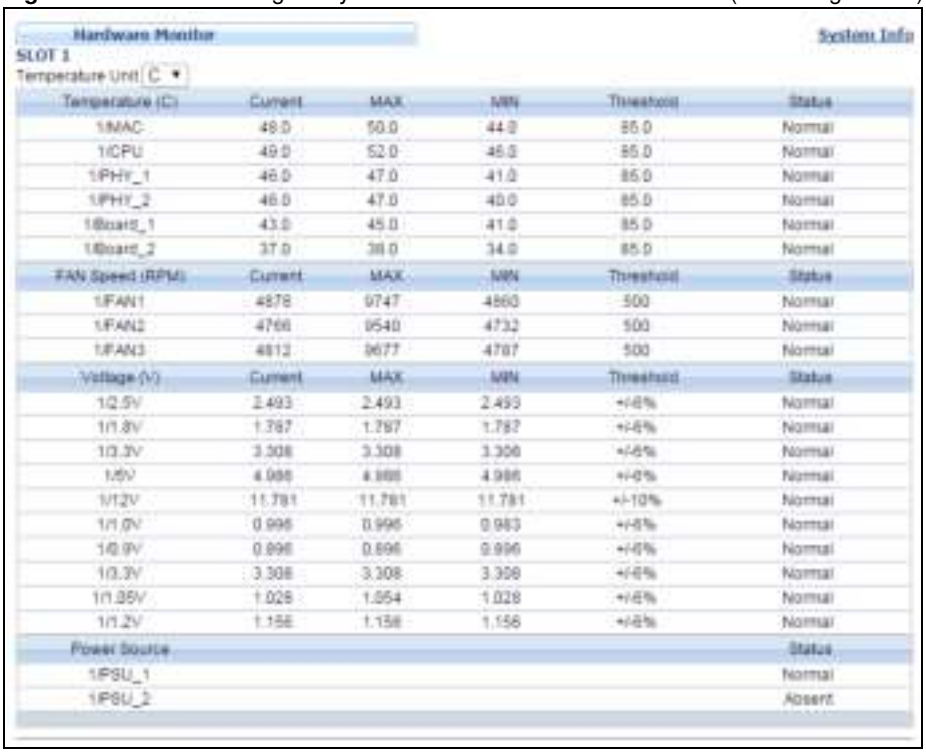
Table 10 Basic Setting > System Info (Standalone and Stacking Modes) (continued)

LABEL	DESCRIPTION
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 **Normal** for temperatures below the threshold and **Error** for those above.
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 (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** 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	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.
Power Source	The power source of the Switch has a sensor that is capable of detecting and reporting if the power source falls out of the normal status.
Status	**Normal** indicates that the power source is within normal status. **Error** indicates that the power source is not within normal status. **Absent** indicates that you do not insert the power module. **Present** indicates that you insert the power module, but there is no available power.
Hardware Status (Stacking Mode)	
Slot	This number identifies the Switch in the stack. Click the number to see more detailed information on the Switch.
Name	This is the system name of the Switch in the stack.
Voltage	This shows if the power supply voltage sensor is within normal tolerance range.
Temperature	This shows if the temperature sensors on the Switch printed circuit board are within normal tolerance range.
Fan	This shows if the fan sensors are within normal tolerance range.
Power Source	This shows whether the power sources are within normal status or not. **Error** indicates that the power source is not within normal status. Otherwise, **Normal** is displayed. You can click the index number in the **Slot** field to view the details.

6.1.1 System Information Stacking Hardware Monitor

Click a slot number in the System Information screen to display more detailed hardware information on a Switch.

Figure 26 Basic Setting > System Info > Hardware Monitor (Stacking Mode)



The following table describes the labels in this screen.

Table 11 Basic Setting > System Info > Hardware Monitor (Stacking Mode)

LABEL	DESCRIPTION
SLOT	This number identifies the Switch in the stack.
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	**BOARD**, **PHY**, **CPU** and **MAC** 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 **Normal** for temperatures below the threshold and **Error** for those above.
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 RPM.
MIN	This field displays this fan's minimum speed measured in RPM. "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.

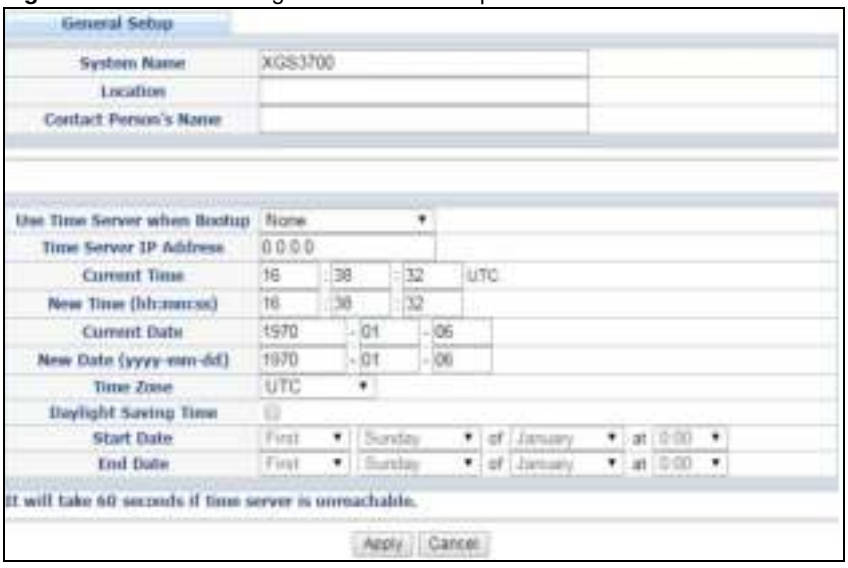
Table 11 Basic Setting > System Info > Hardware Monitor (Stacking Mode) (continued)

LABEL	DESCRIPTION
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	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.
Power Source	The power source of the Switch has a sensor that is capable of detecting and reporting if the power source falls out of the normal status.
Status	**Normal** indicates that the power source is within normal status. **Error** indicates that the power source is not within normal status. **Absent** indicates that you do not insert the power module. **Present** indicates that you insert the power module, but there is no available power.

6.2 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 27 Basic Setting > General Setup



The following table describes the labels in this screen.

Table 12 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Type a descriptive name for identification purposes. This name consists of up to 64 printable ASCII characters; spaces are allowed.
Location	Type the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.

Table 12 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
Contact Person's Name	Type 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	Type 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. When you select the **Daytime (RFC 867)** 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. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** 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.
Time Server IP Address	Type the IP 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:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
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 **Current Date** field after you click **Apply**.
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	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. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: 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 **Second**, **Sunday**, **March** and **2:00**. 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 **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. 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 **First**, **Sunday**, **November** and **2:00**. 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 **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 12 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.3 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 on the same network.

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.

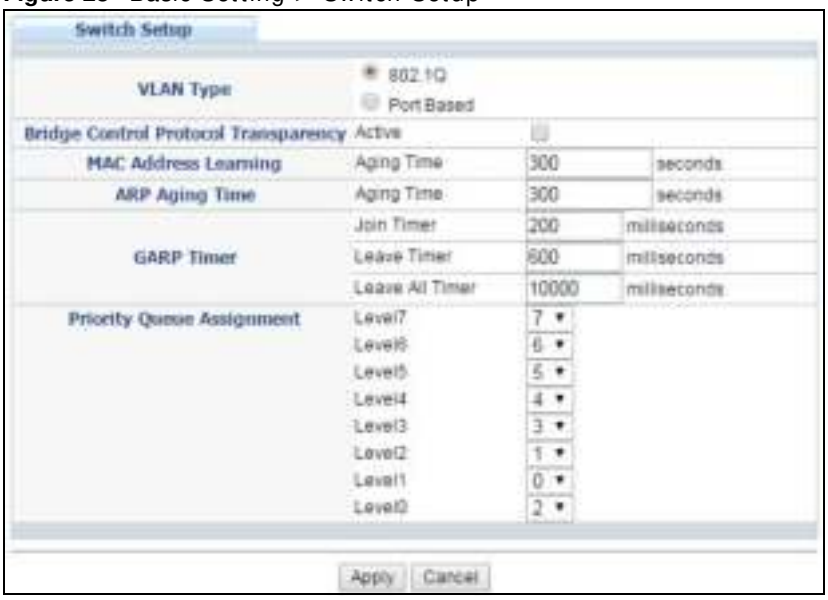
Note: VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 7 on page 101 for information on port-based and 802.1Q tagged VLANs.

6.4 Switch Setup

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 (in Standalone mode). Refer to the chapter on VLAN.

Figure 28 Basic Setting > Switch Setup



The following table describes the labels in this screen.

Table 13 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type (Standalone mode only)	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q** VLAN type or **Port Based** VLAN type in this screen. See Chapter 7 on page 101 for more information. The Switch does not have port-based VLAN available in stacking mode (**Active** is enabled in **Basic Setting > Stacking > Configuration**), so this field does not display in stacking mode.
Bridge Control Protocol Transparency	Select **Active** to allow the Switch to handle bridging control protocols (STP, for example). You also need to define how to treat a BPDU in the **Port Setup** 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 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
ARP Aging Time	
Aging Time	Enter a time from 60 to 1000000 seconds. This is how long dynamically learned ARP entries remain in the ARP table before they age out (and must be relearned). The setting here applies to ARP entries which are newly added in the ARP table after you click **Apply**.
GARP Timer: 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. See Chapter 7 on page 101 for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See Chapter 7 on page 101 for more background information.
Leave Timer	Leave Time sets the duration of the **Leave Period** timer for GVRP in milliseconds. Each port has a single **Leave Period** timer. Leave Time must be two times larger than **Join Timer**; 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.

Table 13 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
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 following 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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.5 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains.

6.5.1 IP Interfaces

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.

On the Switch, an IP address is not bound to any physical ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the Switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

You can configure up to 128 IP domains 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. Each VLAN can only have one management IP address.

Figure 29 Basic Setting > IP Setup

The following table describes the labels in this screen.

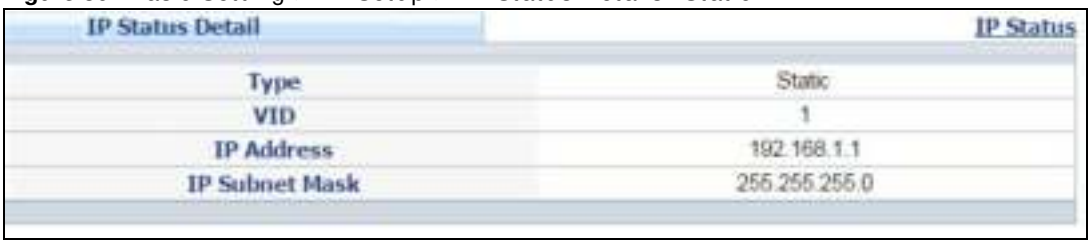
Table 14 Basic Setting > IP Setup

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Type	This shows whether this IP address is dynamically assigned from a DHCP server or manually assigned (**Static**).
Renew	Click this to renew the dynamic IP address.
Release	Click this to release the dynamic IP address.

6.5.2 IP Status Details

Use this screen to view IP status details. Click a number in the **Index** column in the **IP Status** screen to display the screen as shown next.

Figure 30 Basic Setting > IP Setup > IP Status Details: Static

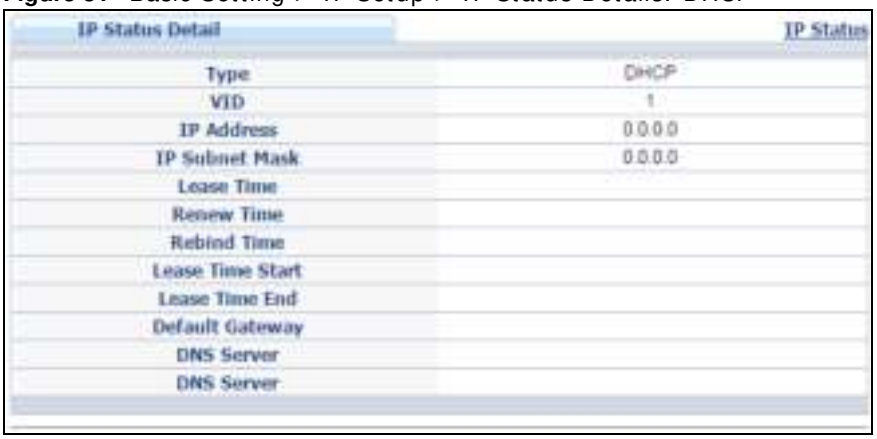


The following table describes the labels in this screen.

Table 15 Basic Setting > IP Setup > IP Status Details: Static

LABEL	DESCRIPTION
Type	This shows whether ths IP address is dynamically assigned from a DHCP server or manually assigned (**Static** or **DHCP**).
VID	This is the VLAN identification number to which an IP routing domain belongs.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.

Figure 31 Basic Setting > IP Setup > IP Status Details: DHCP



The following table describes the labels in this screen.

Table 16 Basic Setting > IP Setup > IP Status Details: DHCP

LABEL	DESCRIPTION
Type	This shows whether ths IP address is dynamically assigned from a DHCP server or manually assigned (**Static** or **DHCP**).
VID	This is the VLAN identification number to which an IP routing domain belongs.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Lease Time	This displays the length of time in seconds that this interface can use the current dynamic IP address from the DHCP server.
Renew Time	This displays the length of time from the lease start that the Switch will request to renew its current dynamic IP address from the DHCP server.
Rebind Time	This displays the length of time from the lease start that the Switch will request to get any dynamic IP address from the DHCP server.
Lease Time Start	This displays the date and time that the current dynamic IP address assignment from the DHCP server began. You should configure date and time in **Basic Setting > General Setup**.
Lease Time End	This displays the date and time that the current dynamic IP address assignment from the DHCP server will end. You should configure date and time in **Basic Setting > General Setup**.
Default Gateway	This displays the IP address of the default gateway assigned by the DHCP server. 0.0.0.0 means no gateway is assigned.
DNS Server	This displays the IP address of the primary and secondary DNS servers assigned by the DHCP server. 0.0.0.0 means no DNS server is assigned.

6.5.3 IP Configuration

Use this screen to configure the default gateway device, the default domain name server and add IP domains.

Figure 32 Basic Setting > IP Setup > IP Configuration

The following table describes the labels in this screen.

Table 17 Basic Setting > IP Setup > IP Configuration

LABEL	DESCRIPTION
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Default Management	Specify which traffic flow (**In-Band** or **Out-of-band**) the Switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source. Select **Out-of-band** to have the Switch send the packets to the management port labelled **MGMT**. This means that device(s) connected to the other port(s) do not receive these packets. Select **In-Band** to have the Switch send the packets to all ports except the management port (labelled **MGMT**) to which connected device(s) do not receive these packets.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Out-of-band Management IP Address Use these fields to set the settings for the out-of-band management port.	
IP Address	Enter the out-of-band management IP address of your Switch in dotted decimal notation. For example, 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation, for example, 255.255.255.0.

Table 17 Basic Setting > IP Setup > IP Configuration (continued)

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.0.254
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
IP Interface Use these fields to create or edit IP routing domains on the Switch.	
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.
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. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click this to create a new entry. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Type	This field displays the type of IP address status.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the Switch.
Cancel	Click **Cancel** to clear the check boxes.

6.6 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 33 Basic Setting > Port Setup (GS3700 Series)

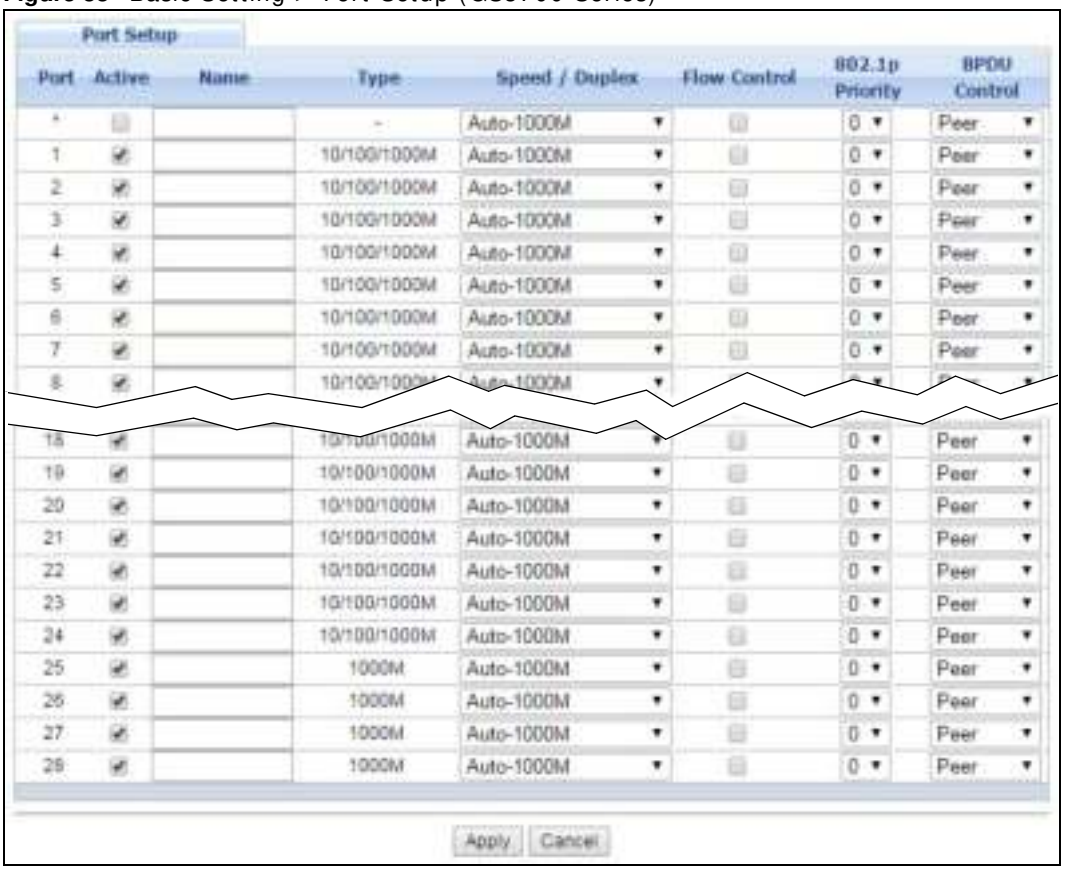


Figure 34 Basic Setting > Port Setup (XGS3700 Series: Standalone mode)

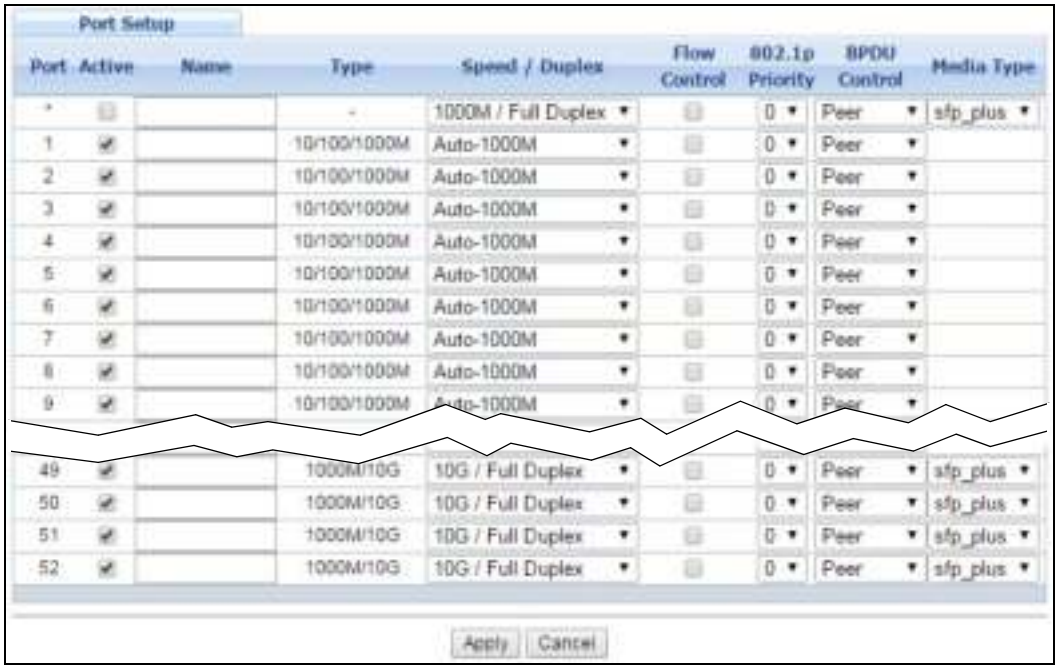
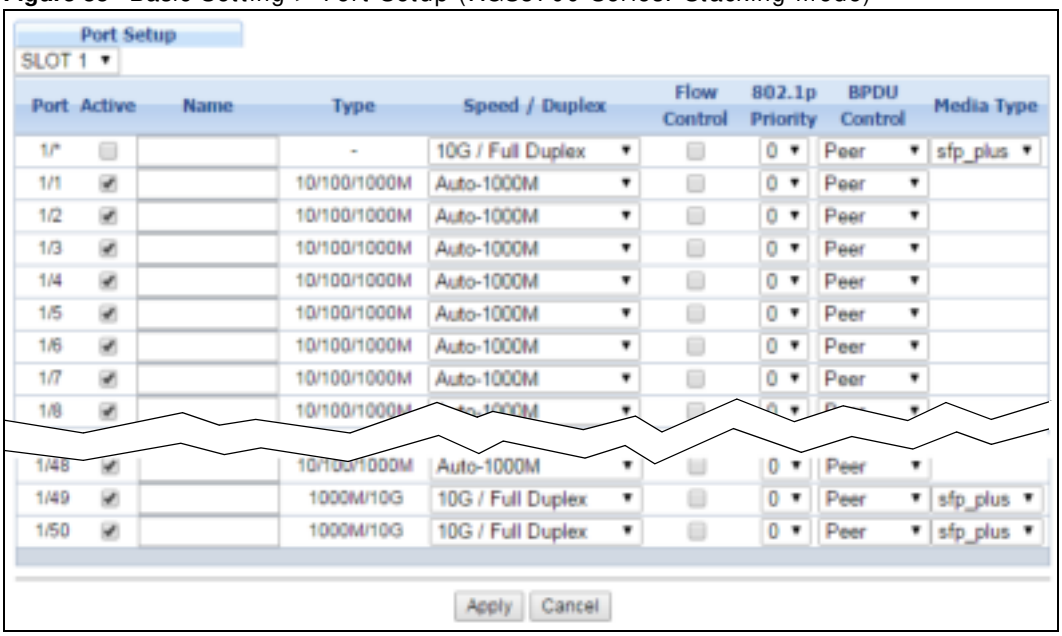


Figure 35 Basic Setting > Port Setup (XGS3700 Series: Stacking mode)



The following table describes the labels in this screen.

Table 18 Basic Setting > Port Setup

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This is the port index number. In stacking mode, the first number is the slot ID and the second is the port number. * means all ports.
*	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.
Name	Type a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitations, the port name may be truncated in some web configurator screens.
Type	This field displays **10M** / **100M**/ **1000M** for a 1000Base-T connection, **1000M** for a 1000Base-X connection, and **10G** for a 10 Gigabit connection (available only on the Switch that has a 10 Gigabit interface).

Table 18 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. The choices are **Auto**, **10M/ Half Duplex**, **10M/ Full Duplex**, **100M/ Half Duplex** and **100M/ Full Duplex** for a 100Base-T connection. **1000M/ Full Duplex** is supported by both 1000Base-T and 1000Base-X connections. **10G/ Full Duplex** is supported by the 10 Gigabit Ethernet connections on the Switch that has a 10 Gigabit interface. Selecting **Auto** (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.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. 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. 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 **Flow Control** to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Table 13 on page 64 for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch **Setup** screen first. Select **Peer** to process any BPDU (Bridge Protocol Data Units) received on this port. Select **Tunnel** to forward BPDUs received on this port. Select **Discard** to drop any BPDU received on this port. Select **Network** to process a BPDU with no VLAN tag and forward a tagged BPDU.
Media Type	On the Switch that has a 10 Gigabit interface, such as the SFP+ slot, you can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC). An SFP+ Direct Attach Copper (DAC) is an SFP+ housing that has no optical module but uses a fixed-length passive copper cable assembly, which reduces cost and power significantly. Select the media type (**sfp_plus** or **dac10g**) of the SFP+ module that is attached to the 10 Gigabit interface.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

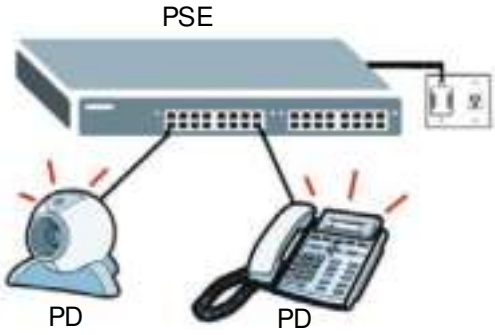
6.7 PoE

Note: The PoE function and the following screens are available for models ending in "HP" only.

The Switch supports both the IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3at High Power over Ethernet (PoE) standards. The Switch is Power Sourcing Equipment (PSE) because it provides a source of power via its Ethernet ports, and each device that receives power through an Ethernet port is a Powered Device (PD).

In the figure below, the IP camera and IP phone get their power directly from the Switch. Aside from minimizing the need for cables and wires, PoE removes the hassle of trying to find a nearby electric outlet to power up devices.

Figure 36 Powered Device Examples



You can also set priorities so that the Switch is able to reserve and allocate power to certain PDs.

Note: The PoE devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

To view the current amount of power that PDs are receiving from the Switch, click **Basic Setting** > **PoE Setup**.

Figure 37 Basic Setting > PoE Setup (Standalone mode)

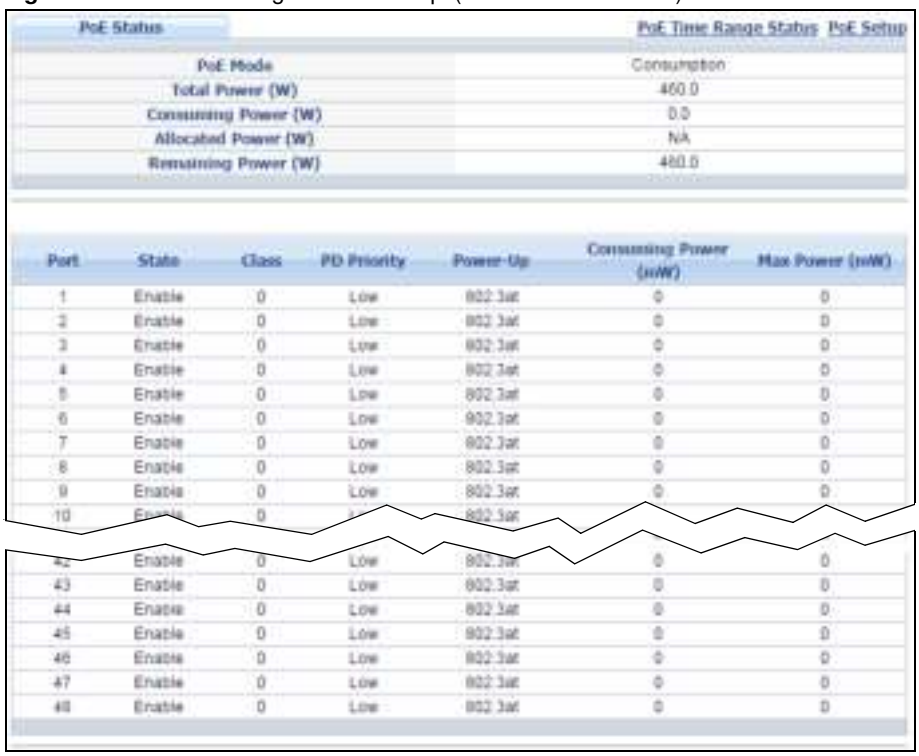
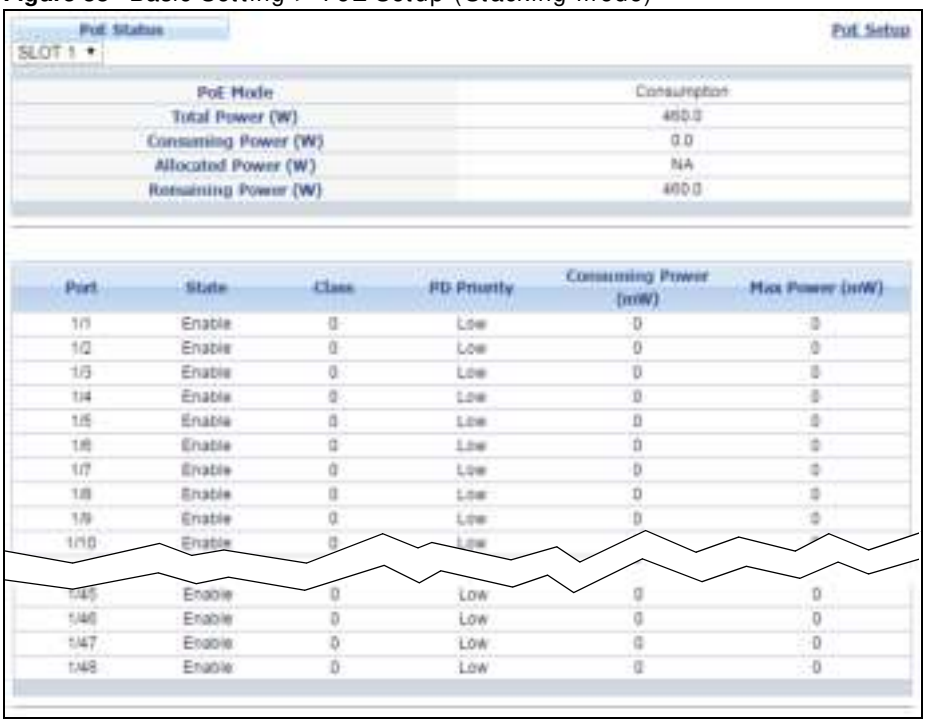


Figure 38 Basic Setting > PoE Setup (Stacking mode)



The following table describes the labels in this screen.

Table 19 Basic Setting > PoE Setup

LABEL	DESCRIPTION
PoE Status	
PoE Mode	This field displays the power management mode used by the Switch, whether it is in **Classification** or **Consumption** mode.
Total Power (W)	This field displays the total power the Switch can provide to the connected PoE-enabled devices on the PoE ports.
Consuming Power (W)	This field displays the total amount of power the Switch is currently supplying to the connected PoE-enabled devices.
Allocated Power (W)	This field displays the total amount of power the Switch has reserved for PoE after negotiating with the connected PoE device(s). **Consuming Power (W)** can be less than or equal but not more than the **Allocated Power (W)**.
Remaining Power (W)	This field displays the amount of power the Switch can still provide for PoE. Note: The Switch must have at least 16 W of remaining power in order to supply power to a PoE device, even if the PoE device needs less than 16 W.
Port (Standalone and stacking mode)	This is the port index number.
State	This field shows which ports can receive power from the Switch. You can set this in the **Basic Setting > PoE Setup** screen. • **Disable** - The PD connected to this port cannot get power. • **Enable** - The PD connected to this port can receive power.

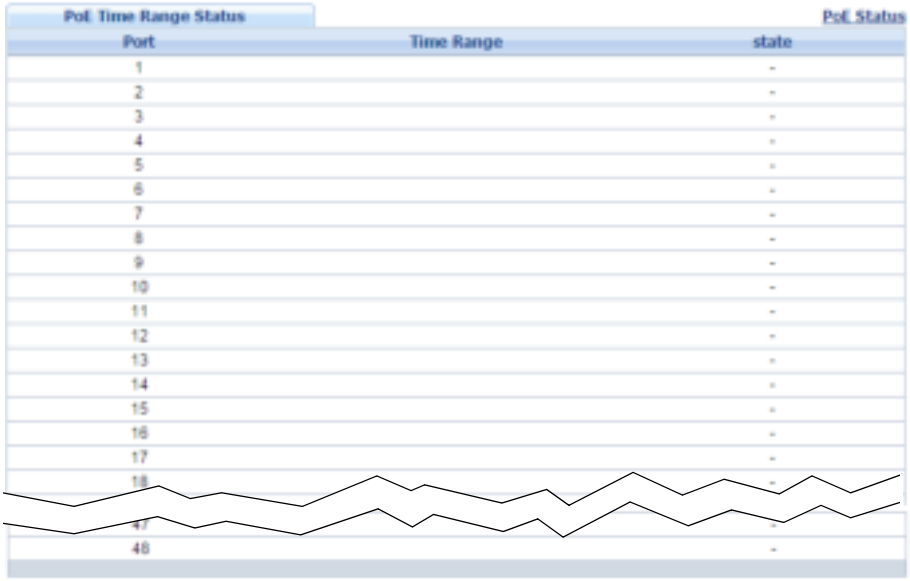
Table 19 Basic Setting > PoE Setup

LABEL	DESCRIPTION
Class	This shows the power classification of the PD. This is a number from 0 to 4, where each value represents a range of power (W) and current (mA) that the PD requires to function. The ranges are as follows. • Class 0 - Default, 0.44 to 12.94 • Class 1 - Optional, 0.44 to 3.84 • Class 2 - Optional, 3.84 to 6.49 • Class 3 - Optional, 6.49 to 12.95 • Class 4 - Reserved (PSEs classify as Class 0) in a switch that supports IEEE 802.3af only. Optional, 12.95 to 25.50 in a switch that supports IEEE 802.3at.
PD Priority	When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority first. • **Critical** has the highest priority. • **High** has the Switch assign power to the port after all critical priority ports are served. • **Low** has the Switch assign power to the port after all critical and high priority ports are served.
Power-Up (Standalone mode)	This field displays the PoE standard the Switch uses to provide power on this port.
Consuming Power (mW)	This field displays the current amount of power consumed by the PD from the Switch on this port.
Max Power (mW)	This field displays the maximum amount of power the PD could use from the Switch on this port.

6.7.1 PoE Time Range Status

Use this screen to see whether PoE is scheduled to be enabled on a port. Click the **PoE Time Range Status** link in the **Basic Setting > PoE Status** screen. The following screen opens.

Figure 39 Basic Setting > PoE Setup > PoE Time Range Status



The following table describes the labels in this screen.

Table 20 Basic Setting > PoE Setup > PoE Time Range Status

LABEL	DESCRIPTION
Port	This is the number of the port on the Switch.
Time Range	This field displays the name of the schedule which is applied to the port. PoE is enabled at the specified time/date.
state	This field displays whether the port can receive power from the Switch (In) or not (Out) currently. It shows - if there is no schedule applied to the port.

6.7.2 PoE Setup

Use this screen to set the priority levels for the Switch in distributing power to PDs.

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

Figure 40 Basic Setting > PoE Setup > PoE Setup (Standalone mode)

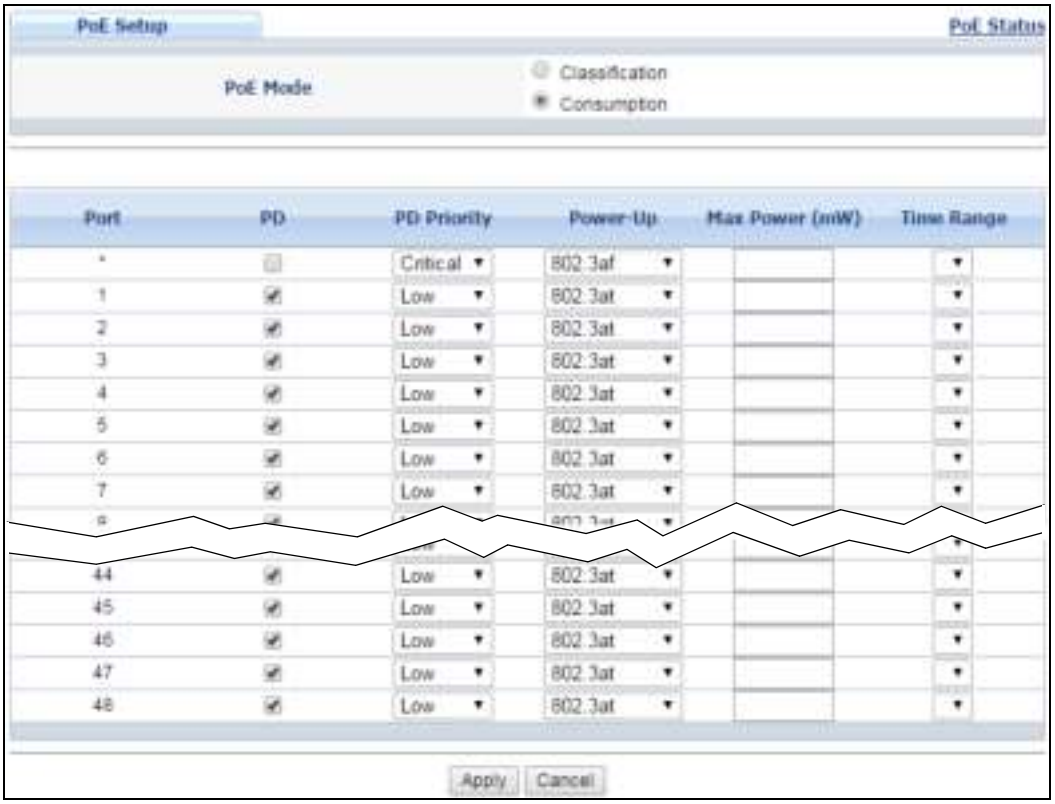
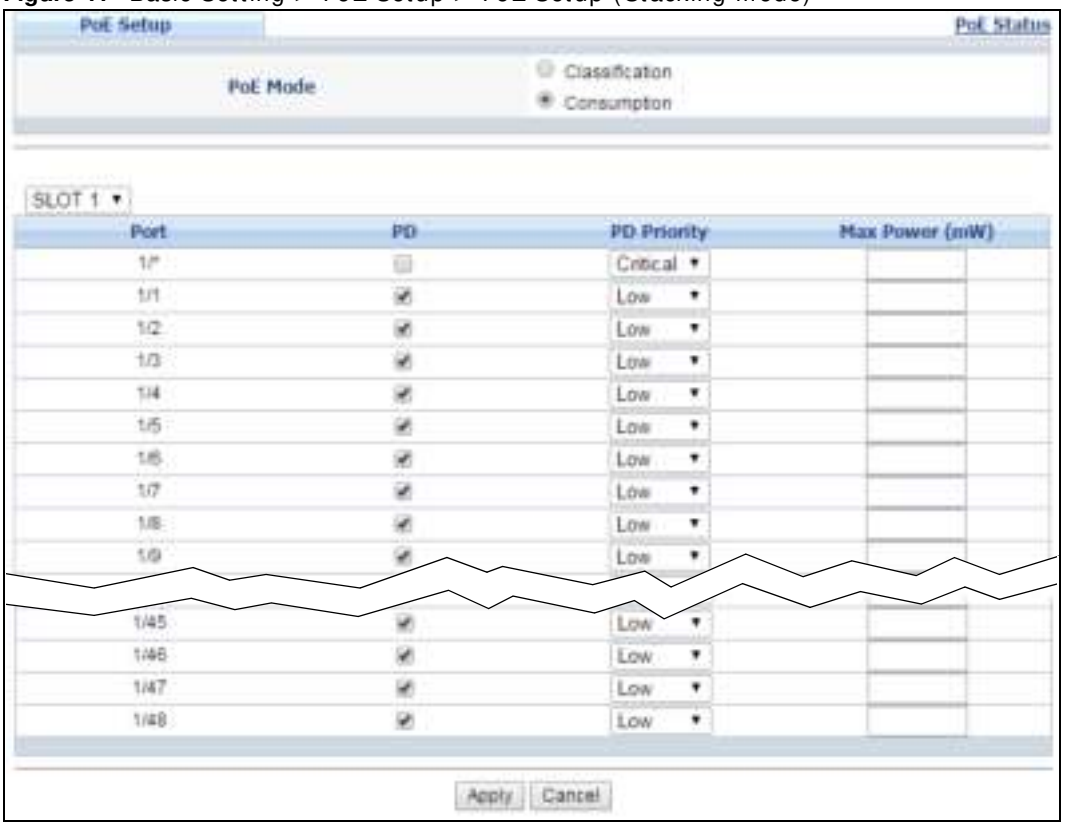


Figure 41 Basic Setting > PoE Setup > PoE Setup (Stacking mode)



The following table describes the labels in this screen.

Table 21 Basic Setting > PoE Setup > PoE Setup

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the Switch to use. • **Classification** - Select this if you want the Switch to reserve the Max Power (mW) to each PD according to the power classification of the PD. If the total power supply available is not enough to supply all connected PDs, then PDs with lower priority do not get power to function. • **Consumption** - Select this if you want the Switch to manage the total power supply so that each connected PD gets a resource. However, the power allocated by the Switch may be less than the **Max Power (mW)** of the PD. PDs with higher priority also get more power than those with lower priority levels.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or Stacking mode)	This is the port index number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
PD	Select this to provide power to a PD connected to the port. If left unchecked, the PD connected to the port cannot receive power from the Switch.

Table 21 Basic Setting > PoE Setup > PoE Setup (continued)

LABEL	DESCRIPTION
PD Priority	This field is not available for the SFP or SFP+ ports. When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority. Select **Critical** to give the PD connected to this port the highest priority. Select **High** to set the Switch to assign the remaining power to the port after all critical priority ports are served. Select **Low** to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.
Power-Up (Standalone mode)	Set how the Switch provides power to a connected PD at power-up. **802.3af** - the Switch follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up. **Legacy** - the Switch can provide power to the connected PDs that require high inrush currents at power-up. Inrush current is the maximum, instantaneous input current drawn by the PD when first turned on. **Pre-802.3at** - the Switch initially offers power on the port according to the IEEE 802.3af standard, and then switches to support the IEEE 802.3at standard within 75 milliseconds after a PD is connected to the port. Select this option if the Switch is performing 2-event Layer-1 classification (PoE+ hardware classification) or the connected PD is NOT performing Layer 2 power classification using Link Layer Discovery Protocol (LLDP). **802.3at** - the Switch supports the IEEE 802.3at High Power over Ethernet standard and can supply power of up to 30W per Ethernet port. IEEE 802.3at is also known as PoE+ or PoE Plus. An IEEE 802.3at compatible device is referred to as Type 2. Power Class 4 (High Power) can only be used by Type 2 devices. If the connected PD requires a Class 4 current when it is turned on, it will be powered up in this mode.
Max Power (mW)	Set the maximum amount of power (from 1000 to 33000) the PD could use from the Switch on this port. Otherwise, leave the field blank to allow the connected PD to use power up to 33W in **Consumption** mode and 30W in **Classification** mode.
Time Range (Standalone mode)	Select a pre-defined schedule (created using the **Advanced Application > Time Range** screen) to control when the Switch enables PoE to provide power on the port. If you leave this field blank, PoE is disabled on the port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Note: If the priority settings for two or more PoE ports are the same and the power budget is not enough, the ports will shut down randomly. We strongly recommend you set the priority for each PoE port to make sure the high priority ports get power.

Note: The total power available varies by Switch. Use the `show pwr` command to see the total power available for your Switch. The number of ports that can be powered by PoE is the (total power available) / (maximum power available per port).

In **Consumption** mode the power available per port is from 1 to 33 watts. Configure the maximum power available per port in the **Max Power (mW)** field in **Basic Setting > PoE Status > PoE Setup**.

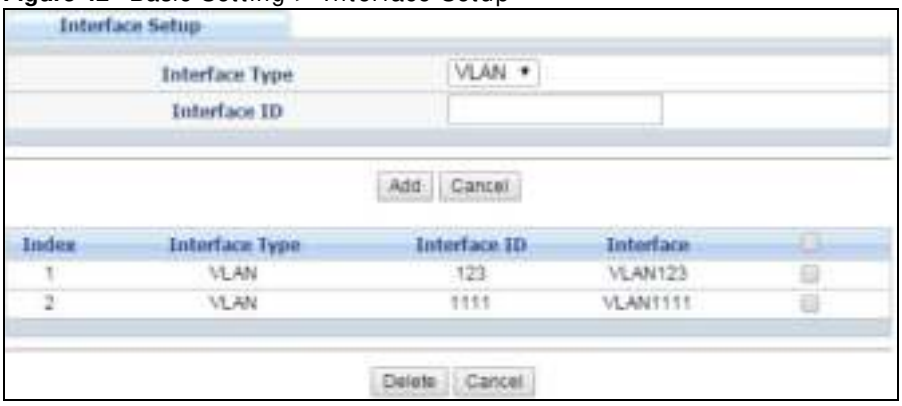
In **Classification** mode the power available per port is from 1 to 30 watts. The maximum power available per port depends on the the power classification of the connected PD - see the **Class** field in **Basic Setting > PoE Status > PoE Setup**.

6.8 Interface Setup

An IPv6 address is configured on a per-interface basis. The interface can be a physical interface (for example, an Ethernet port) or a virtual interface (for example, a VLAN). The Switch supports the VLAN interface type for IPv6 at the time of writing.

Use this screen to set IPv6 interfaces on which you can configure an IPv6 address to access and manage the Switch. Click **Basic Setting** > **Interface Setup** in the navigation panel to display the configuration screen.

Figure 42 Basic Setting > Interface Setup



The following table describes the labels in this screen.

Table 22 Basic Setting > Interface Setup

LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. Note: To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **Advanced Setup > VLAN** screens.
Add	Click this to create a new entry. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

Table 22 Basic Setting > Interface Setup (continued)

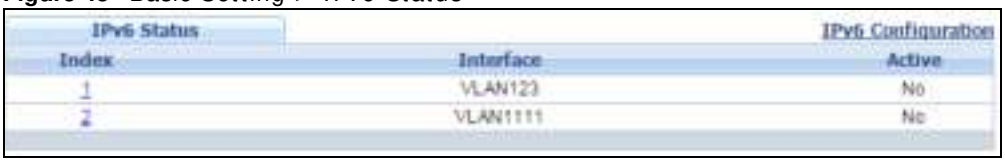
LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Interface Type	This field displays the type of interface.
Interface ID	This field displays the identification number of the interface.
Interface	This field displays the interface's descriptive name which is generated automatically by the Switch. The name is from a combination of the interface type and ID number.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

6.9 IPv6

Use this screen to view the IPv6 interface status and configure Switch's management IPv6 addresses. See Appendix B on page 517 for more information about IPv6.

Click **Basic Setting** > **IPv6** in the navigation panel to display the IPv6 status screen as shown next.

Figure 43 Basic Setting > IPv6 Status



The following table describes the labels in this screen.

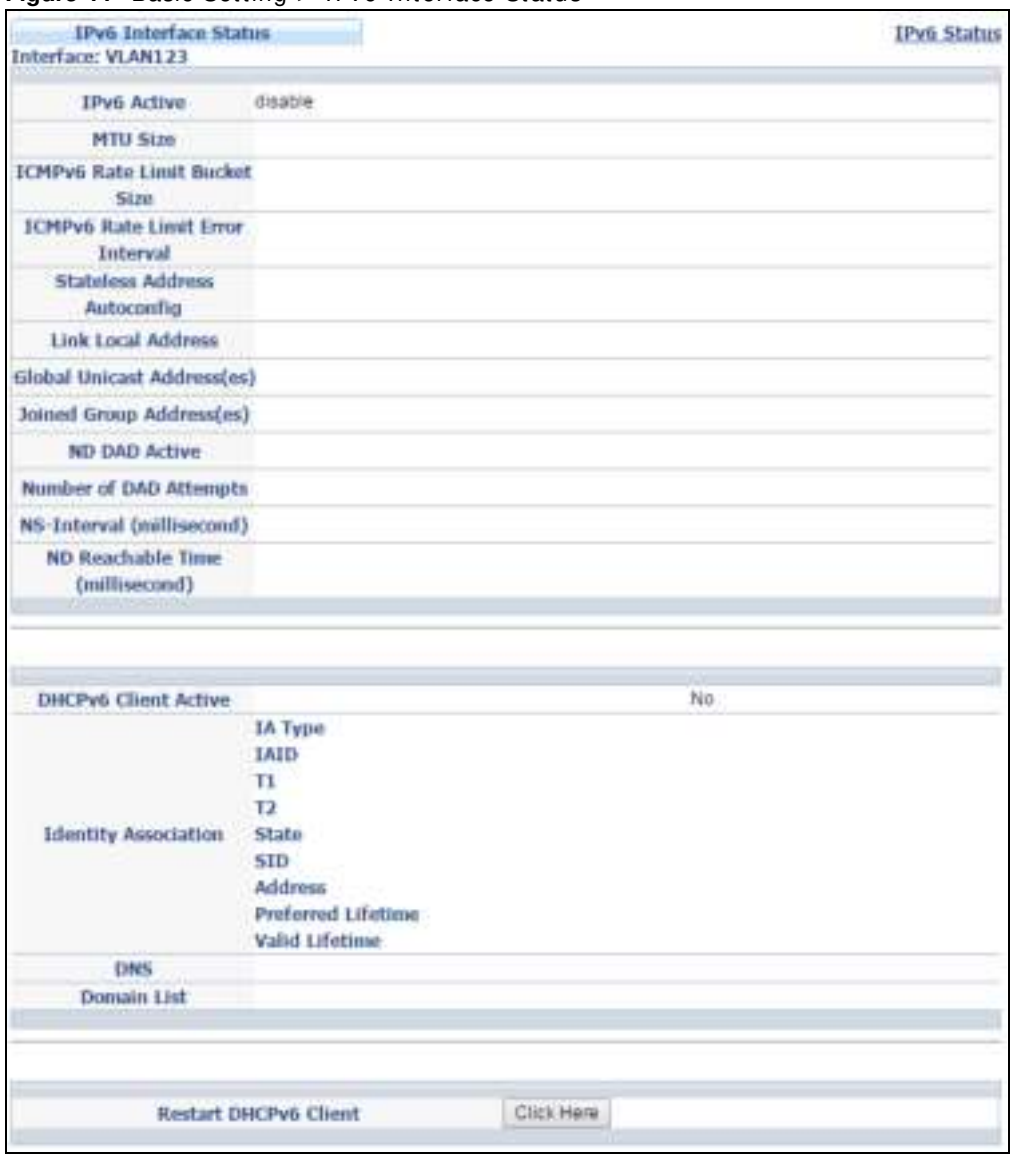
Table 23 Basic Setting > IPv6 Status

LABEL	DESCRIPTION
Index	This field displays the index number of an IPv6 interface. Click on an index number to view more interface details.
Interface	This is the name of the IPv6 interface you created.
Active	This field displays whether the IPv6 interface is activated or not.

6.9.1 IPv6 Interface Status

Use this screen to view a specific IPv6 interface status and detailed information. Click an interface index number in the **Basic Setting** > **IPv6** screen. The following screen opens.

Figure 44 Basic Setting > IPv6 Interface Status



The following table describes the labels in this screen.

Table 24 Basic Setting > IPv6 Interface Status

LABEL	DESCRIPTION
IPv6 Active	This field displays whether the IPv6 interface is activated or not.
MTU Size	This field displays the Maximum Transmission Unit (MTU) size for IPv6 packets on this interface.
ICMPv6 Rate Limit Bucket Size	This field displays the maximum number of ICMPv6 error messages which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.
ICMPv6 Rate Limit Error Interval	This field displays the time period (in milliseconds) during which ICMPv6 error messages of up to the bucket size can be transmitted. 0 means no limit.
Stateless Address Autoconfig	This field displays whether the Switch's interface can automatically generate a link-local address via stateless autoconfiguration.

Table 24 Basic Setting > IPv6 Interface Status (continued)

LABEL	DESCRIPTION
Link Local Address	This field displays the Switch's link-local IP address and prefix generated by the interface. It also shows whether the IP address is preferred, which means it is a valid address and can be used as a sender or receiver address.
Global Unicast Address(es)	This field displays the Switch's global unicast address to identify this interface.
Joined Group Address(es)	This field displays the IPv6 multicast addresses of groups the Switch's interface joins.
ND DAD Active	This field displays whether Neighbor Discovery (ND) Duplicate Address Detection (DAD) is enabled on the interface.
Number of DAD Attempts	This field displays the number of consecutive neighbor solicitations the Switch sends for this interface.
NS-Interval (millisecond)	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
ND Reachable Time (millisecond)	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.
DHCPv6 Client Active	This field displays whether the Switch acts as a DHCPv6 client to get an IPv6 address from a DHCPv6 server.
Identity Association	An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface.
IA Type	The IA type is the type of address in the IA. Each IA holds one type of address. **IA_NA** means an identity association for non-temporary addresses and **IA_TA** is an identity association for temporary addresses.
IAID	Each IA consists of a unique IAID and associated IP information.
T1	This field displays the DHCPv6 T1 timer. After T1, the Switch sends the DHCPv6 server a Renew message. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire.
T2	This field displays the DHCPv6 T2 timer. If the time T2 is reached and the server does not respond, the Switch sends a Rebind message to any available server.
State	This field displays the state of the TA. It shows • **Active** when the Switch obtains addresses from a DHCpv6 server and the TA is created. • **Renew** when the TA's address lifetime expires and the Switch sends out a Renew message. • **Rebind** when the Switch doesn't receive a response from the original DHCPv6 server and sends out a Rebind message to another DHCPv6 server.
SID	This field displays the DHCPv6 server's unique ID.
Address	This field displays the Switch's global address which is assigned by the DHCPv6 server.
Preferred Lifetime	This field displays how long (in seconds) that the global address remains preferred.
Valid Lifetime	This field displays how long (in seconds) that the global address is valid.
DNS	This field displays the DNS server address assigned by the DHCPv6 server.
Domain List	This field displays the address record when the Switch queries the DNS server to resolve domain names.
Restart DHCPv6 Client	Click **Click Here** to send a new DHCP request to the DHCPv6 server and update the IPv6 address and DNS information for this interface.

6.9.2 IPv6 Configuration

Use this screen to configure IPv6 settings on the Switch. Click the **IPv6 Configuration** link in the **Basic Setting** > **IPv6** screen. The following screen opens.

Figure 45 Basic Setting > IPv6 > IPv6 Configuration

The following table describes the labels in this screen.

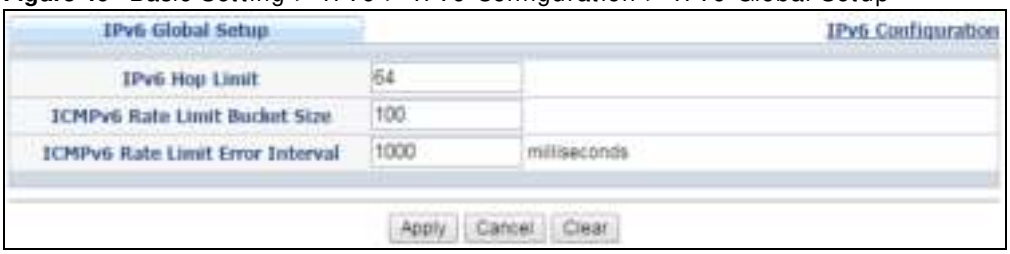
Table 25 Basic Setting > IPv6 > IPv6 Configuration

LABEL	DESCRIPTION
IPv6 Global Setup	Click the link to go to a screen where you can configure the global IPv6 settings on the Switch.
IPv6 Interface Setup	Click the link to go to a screen where you can enable an IPv6 interface on the Switch.
IPv6 Addressing	
IPv6 Link-Local Address Setup	Click the link to go to a screen where you can configure the IPv6 link-local address for an interface.
IPv6 Global Address Setup	Click the link to go to a screen where you can configure the IPv6 global address for an interface.
IPv6 Neighbor Discovery	
IPv6 Neighbor Discovery Setup	Click the link to go to a screen where you can configure the IPv6 neighbor discovery settings.
IPv6 Router Discovery Setup	Click the link to go to a screen where you can configure the IPv6 router discovery settings.
IPv6 Prefix Setup	Click the link to go to a screen where you can configure the Switch's IPv6 prefix list.
IPv6 Neighbor Setup	Click the link to go to a screen where you can create a static IPv6 neighbor entry in the Switch's IPv6 neighbor table.
DHCPv6 Client Setup	Click the link to go to a screen where you can configure the Switch DHCP settings.

6.9.3 IPv6 Global Setup

Use this screen to configure the global IPv6 settings. Click the link next to **IPv6 Global Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 46 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup



The following table describes the labels in this screen.

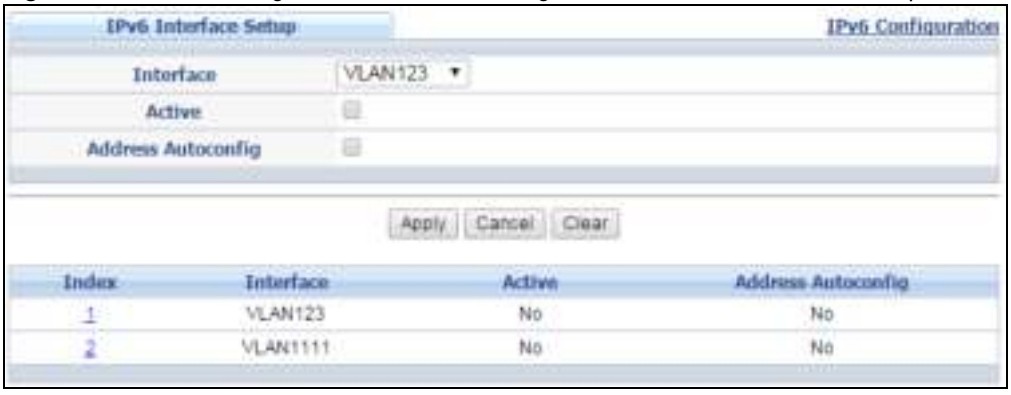
Table 26 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

LABEL	DESCRIPTION
IPv6 Hop Limit	Specify the maximum number of hops (from 1 to 255) in router advertisements. This is the maximum number of hops on which an IPv6 packet is allowed to transmit before it is discarded by an IPv6 router, which is similar to the TTL field in IPv4.
ICMPv6 Rate Limit Bucket Size	Specify the maximum number of ICMPv6 error messages (from 1 to 200) which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.
ICMPv6 Rate Limit Error Interval	Specify the time period (from 0 to 2147483647 milliseconds) during which ICMPv6 error messages of up to the bucket size can be transmitted. 0 means no limit.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.

6.9.4 IPv6 Interface Setup

Use this screen to turn on or off an IPv6 interface and enable stateless autoconfiguration on it. Click the link next to **IPv6 Interface Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 47 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup



The following table describes the labels in this screen.

Table 27 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

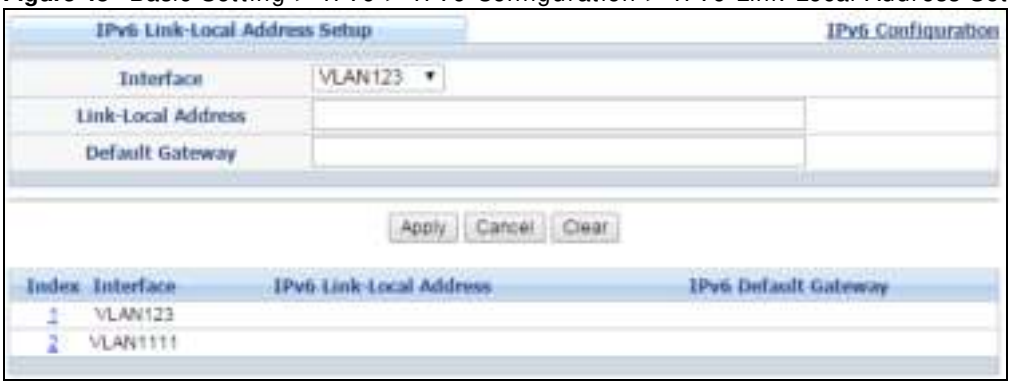
LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Active	Select this option to enable the interface.
Address Autoconfig	Select this option to allow the interface to automatically generate a link-local address via stateless autoconfiguration.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Active	This field displays whether the IPv6 interface is activated or not.
Address Autoconfig	This field displays whether stateless autoconfiguration is enabled on the interface.

6.9.5 IPv6 Link-Local Address Setup

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.

Use this screen to configure the interface's link-local address and default gateway. Click the link next to **IPv6 Link-Local Address Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 48 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup



The following table describes the labels in this screen.

Table 28 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Link-Local Address	Manually configure a static IPv6 link-local address for the interface.

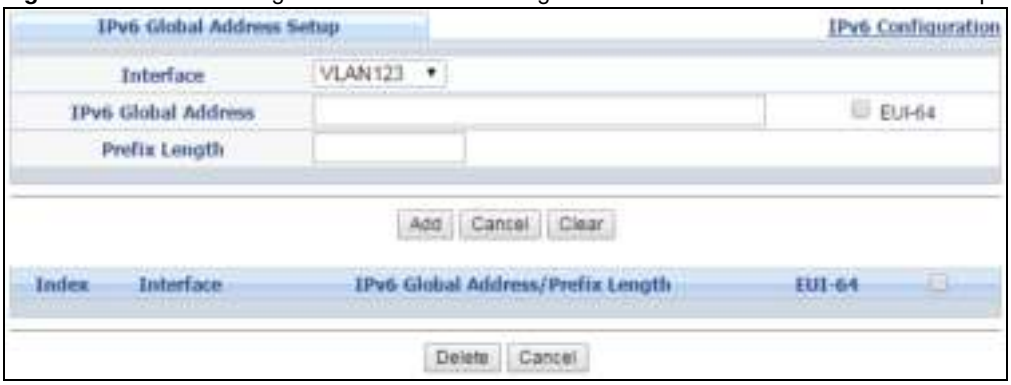
Table 28 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup (continued)

LABEL	DESCRIPTION
Default Gateway	Set the default gateway IPv6 address for the interface. When an interface cannot find a routing information for a frame's destination, it forwards the packet to the default gateway.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IPv6 Link-Local Address	This is the static IPv6 link-local address for the interface.
IPv6 Default Gateway	This is the default gateway IPv6 address for the interface.

6.9.6 IPv6 Global Address Setup

Use this screen to configure the interface's IPv6 global address. Click the link next to **IPv6 Global Address Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 49 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup



The following table describes the labels in this screen.

Table 29 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IPv6 Global Address	Manually configure a static IPv6 global address for the interface.
Prefix Length	Specify an IPv6 prefix length that specifies how many most significant bits (start from the left) in the address compose the network address.
EUI-64	Select this option to have the interface ID be generated automatically using the EUI-64 format.
Add	Click **Add** to create a new entry or update an existing one.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.

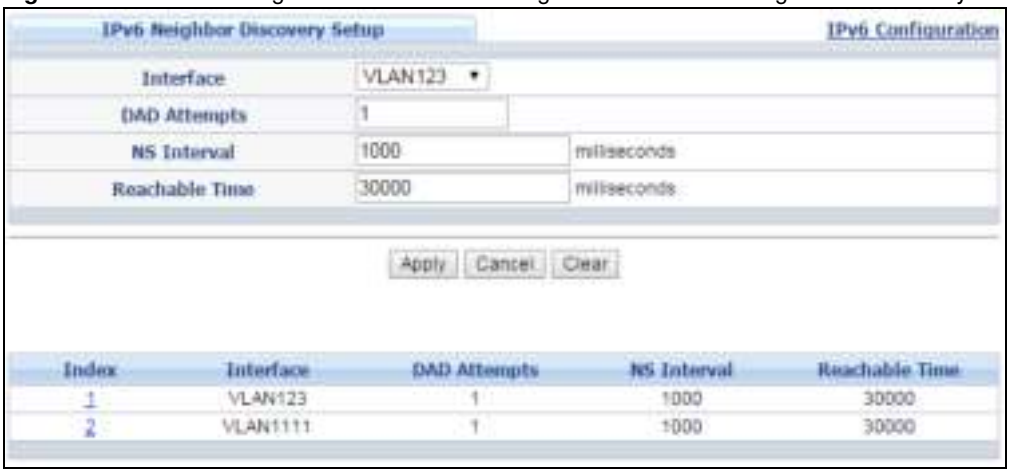
Table 29 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup (continued)

LABEL	DESCRIPTION
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IPv6 Global Address/ Prefix Length	This field displays the IPv6 global address and prefix length for the interface.
EUI-64	This shows whether the interface ID of the global address is generated using the EUI-64 format.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click **Delete** to remove the selected entry(ies) from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

6.9.7 IPv6 Neighbor Discovery Setup

Use this screen to configure neighbor discovery settings for each interface. Click the link next to **IPv6 Neighbor Discovery Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 50 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup



The following table describes the labels in this screen.

Table 30 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
DAD Attempts	The Switch uses Duplicate Address Detection (DAD) with neighbor solicitation and advertisement messages to check whether an IPv6 address is already in use before assigning it to an interface, such as the link-local address it creates through stateless address autoconfiguration. Specify the number of consecutive neighbor solicitations (from 0 to 600) the Switch sends for this interface. Enter 0 to turn off DAD.
NS Interval	Specify the time interval (from 1000 to 3600000 milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	Specify how long (from 1000 to 3600000 milliseconds) a neighbor is considered reachable for this interface.

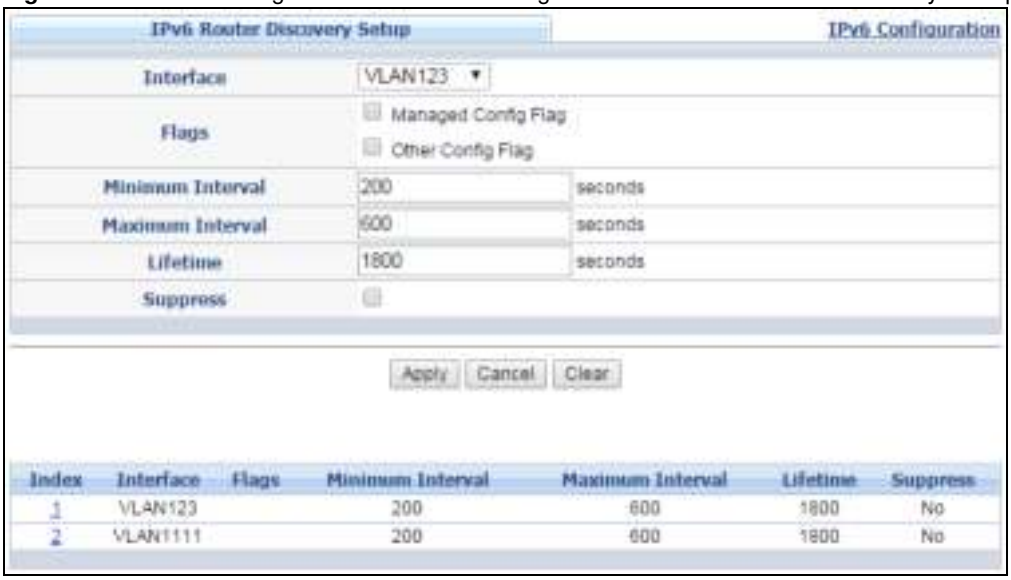
Table 30 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
DAD Attempts	This field displays the number of consecutive neighbor solicitations the Switch sends for this interface.
NS Interval	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.

6.9.8 IPv6 Router Discovery Setup

Use this screen to configure router discovery settings for each interface. Click the link next to **IPv6 Router Discovery Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 51 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup



The following table describes the labels in this screen.

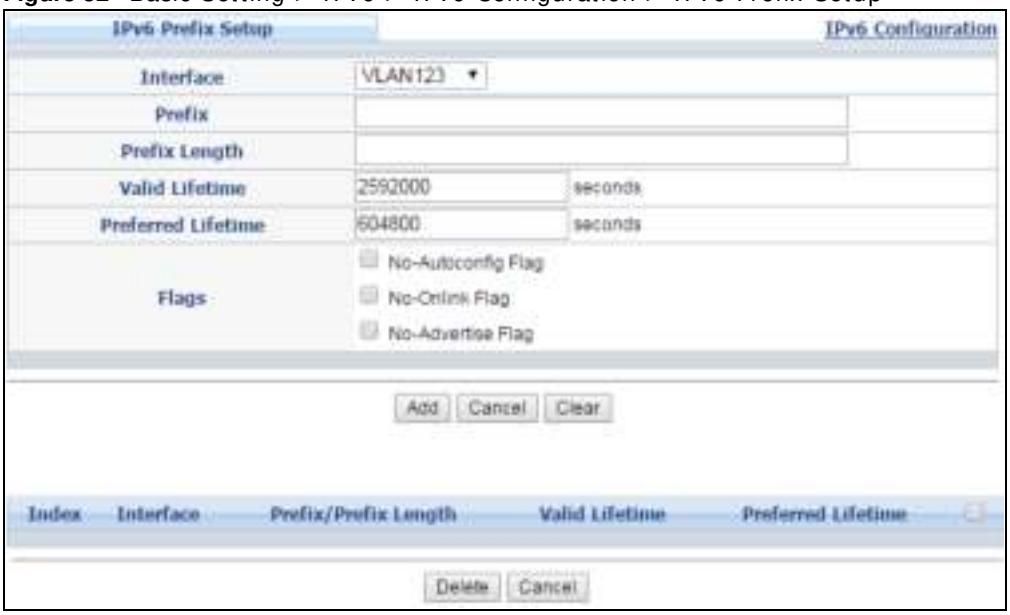
Table 31 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Flags	Select the **Managed Config Flag** option to have the Switch set the "managed address configuration" flag (the M flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain IPv6 stateful addresses. Select the **Other Config Flag** option to have the Switch set the "Other stateful configuration" flag (the O flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain additional configuration settings, such as DNS information. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain additional configuration settings.
Minimum Interval	Specify the minimum time interval (from 3 to 1350 seconds) at which the Switch sends router advertisements for this interface. Note: The minimum time interval cannot be greater than three-quarters of the maximum time interval.
Maximum Interval	Specify the maximum time interval (from 4 to 1800 seconds) at which the Switch sends router advertisements for this interface.
Lifetime	Specify how long (from 0 to 9000 seconds) the router in router advertisements can be used as a default router for this interface.
Suppress	Select this option to set the Switch to not send router advertisements and responses to router solicitations on this interface.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Flags	This field displays whether IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses (**M**) and/or additional configuration settings (**O**).
Minimum Interval	This field displays the minimum time interval at which the Switch sends router advertisements for this interface.
Maximum Interval	This field displays the maximum time interval at which the Switch sends router advertisements for this interface.
Lifetime	This field displays how long the router in router advertisements can be used as a default router for this interface.
Suppress	This field displays whether the Switch sends router advertisements and responses to router solicitations on this interface (**No**) or not (**Yes**).

6.9.9 IPv6 Prefix Setup

Use this screen to configure the Switch's IPv6 prefix list for each interface. Click the link next to **IPv6 Prefix Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 52 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup



The following table describes the labels in this screen.

Table 32 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Prefix	Set the IPv6 prefix that the Switch includes in router advertisements for this interface.
Prefix Length	Set the prefix length that the Switch includes in router advertisements for this interface.
Valid Lifetime	Specify how long (from 0 to 4294967295 seconds) the prefix is valid for on-link determination.
Preferred Lifetime	Specify how long (from 0 to 4294967295 seconds) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The preferred lifetime cannot exceed the valid lifetime.
Flags	Select **No-Autoconfig Flag** to not allow IPv6 hosts to use this prefix for stateless address autoconfiguration. Select **No-Onlink Flag** to not allow the specified prefix to be used for on-link determination. Select **No-Advertise Flag** to set the Switch to not include the specified IPv6 prefix, prefix length in router advertisements for this interface.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Prefix/Prefix Length	This field displays the IPv6 prefix and prefix length that the Switch includes in router advertisements for this interface.
Valid Lifetime	This field displays the IPv6 prefix valid lifetime.

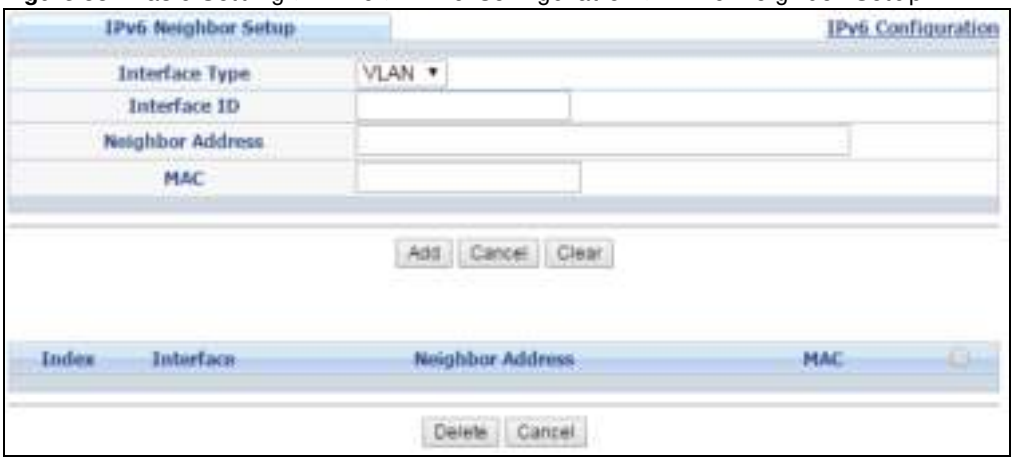
Table 32 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup (continued)

LABEL	DESCRIPTION
Preferred Lifetime	This field displays the preferred lifetime of an IPv6 address generated from the prefix.
Delete	Check the entry(ies) that you want to remove in the **Delete** column and then click **Delete** to remove the selected entry(ies) from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

6.9.10 IPv6 Neighbor Setup

Use this screen to create a static IPv6 neighbor entry in the Switch's IPv6 neighbor table to store the neighbor information permanently. Click the link next to **IPv6 Neighbor Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 53 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup



The following table describes the labels in this screen.

Table 33 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. Note: A static IPv6 neighbor entry displays in the **Management > Neighbor Table** screen only when the interface ID is also created in the **Basic Setup > Interface Setup** screen. Note: To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **Advanced Setup > VLAN** screens.
Neighbor Address	Specify the IPv6 address of the neighboring device which can be reached through the interface.
MAC	Specify the MAC address of the neighboring device which can be reached through the interface.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.

Table 33 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Neighbor Address	This field displays the IPv6 address of the neighboring device which can be reached through the interface
MAC	This field displays the MAC address of the neighboring device which can be reached through the interface.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click **Delete** to remove the selected entry(ies) from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

6.9.11 DHCPv6 Client Setup

Use this screen to configure the Switch's DHCP settings when it is acting as a DHCPv6 client. Click the link next to **IPv6 Neighbor Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 54 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

The following table describes the labels in this screen.

Table 34 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IA Type	Select **IA-NA** to set the Switch to get a non-temporary IP address from the DHCPv6 server for this interface. Optionally, you can also select **Rapid-Commit** to have the Switch send its DHCPv6 Solicit message with a Rapid Commit option to obtain information from the DHCPv6 server by a rapid two-message exchange. The Switch discards any Reply messages that do not include a Rapid Commit option. The DHCPv6 server should also support the Rapid Commit option to have it work well.

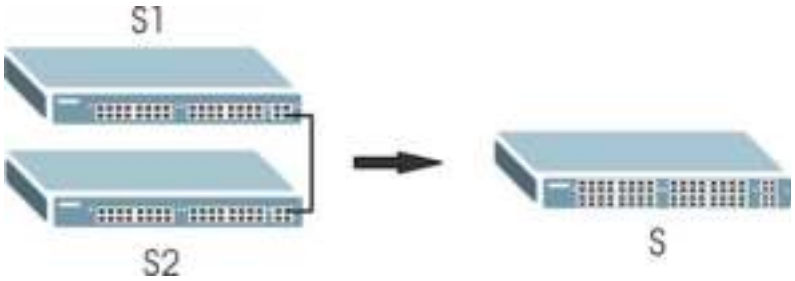
Table 34 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup (continued)

LABEL	DESCRIPTION
Options	Select **DNS** to have the Switch obtain DNS server IPv6 addresses and/or select **Domain-List** to have the Switch obtain a list of domain names from the DHCP server.
Information Refresh Minimum	Specify the time interval (from 600 to 4294967295 seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IA-NA	This field displays whether the Switch obtains a non-temporary IP address from the DHCPv6 server.
Rapid-Commit	This field displays whether the Switch obtains information from the DHCPv6 server by a rapid two-message exchange.
DNS	This field displays whether the Switch obtains DNS server IPv6 addresses from the DHCPv6 server.
Domain-List	This field displays whether the Switch obtains a list of domain names from the DHCP server.
Information Refresh Minimum	This field displays the time interval (in seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.

6.10 Stacking

Stacking is directly connecting Switches to form a larger system that behaves as a single Switch or a virtual chassis with increased port density.

Figure 55 Switch Stacking Concept



The last two SFP ports of your Switch are dedicated for Switch stacking. These are the Switches that support stacking at the time of writing.

Table 35 Switch Stacking

MODELS WITH STACKING SUPPORT
XGS3700-24
XGS3700-24HP

Table 35 Switch Stacking

MODELS WITH STACKING SUPPORT
XGS3700-48
XGS3700-48HP

Note: Up to 8 Switches per stack are allowed.

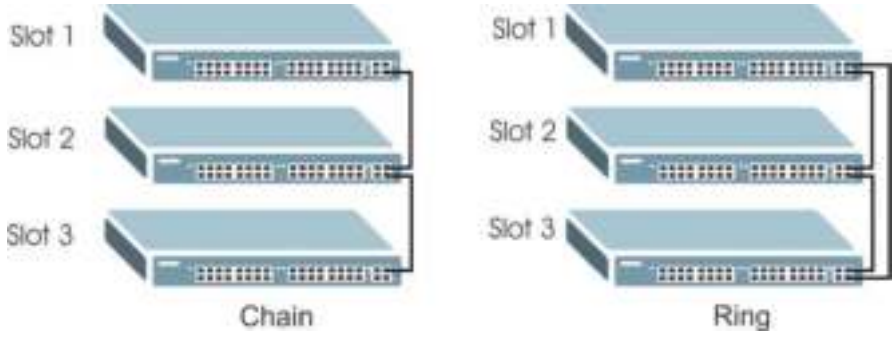
You can manage each Switch in the stack from a master Switch using its web configurator or console. Each Switch supports up to two stacking channels. Use the master Switch to assign a 'slot ID' for each 'linecard' non-master Switch. 'Slot' refers to a Switch in the the 'virtual chassis' stack.

The advantages of stacking are:

- High port density - for example, two 24-port Switches can become one 48-port logical Switch
- Centralized management - log into a single IP address of the master switch to control all Switches in the stacking system using the web configurator, CLI, SNMP or FTP
- Redundancy - Data redundancy allows traffic to be forwarded even if one Switch in the stack fails. Management redundancy lets you still manage the stack even if one Switch in the stack fails
- Modularity and hot-swappable - you can add, remove, or replace Switches to increase or decrease the stack with minimum disruption to ongoing network traffic.

You can build a Switch stack using a ring or chain topology. In a ring topology, the last Switch is connected to the first.

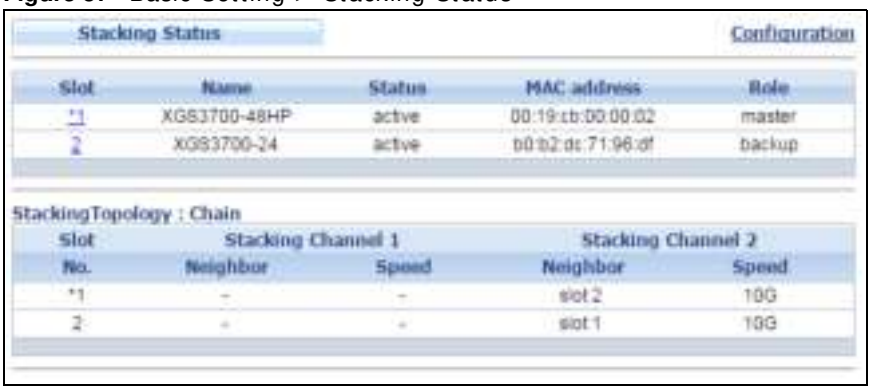
Figure 56 Stacking Topology



6.10.1 Stacking Status

Click **Basic Setting** > **Stacking** in the navigation panel to display the **Stacking Status** screen as shown next.

Figure 57 Basic Setting > Stacking Status



The following table describes the labels in this screen.

Table 36 Basic Setting > Stacking > Stacking Status

LABEL	DESCRIPTION
Slot	'Slot' refers to a Switch in the the 'virtual chassis' stack. This field displays the slot ID of the stacked Switch. You can click the ID number to go to the **Stacking Slot Status** screen.
Name	This field displays the model name of the stacked Switch.
Status	This field displays whether the stacked Switch is active or inactive in a stack system. **Init** means the slot ID is initialized by the master Switch.
MAC address	This field displays the MAC address of the stacked Switch.
Role	This field displays whether the Switch is a master, backup or linecard. There's only one master and one backup Switch in the stacking model; all others are linecard Switches.
Stacking Topology: Ring/Chain	
Slot No.	This field displays the slot ID number of the stacked Switch.
Stacking Channel1	
Neighbor	This field displays the neighbor Switch that is connected using slot channel 1 of the Switch.
Speed	This field displays the Ethernet speed of stacking channel 1 of the Switch.
Stacking Channel2	
Neighbor	This field displays the neighbor Switch that is connected to slot channel 2 of the Switch.
Speed	This field displays the Ethernet speed of stacking channel 2 of the Switch.

6.10.2 Stacking Slot

Click **Basic Setting** > **Stacking** > **Stacking Status** > **Slot number** in the navigation panel to display the **Stacking Slot Status** screen as shown next.

Figure 58 Basic Setting > Stacking > Stacking Status > Slot number

The following table describes the labels in this screen.

Table 37 Basic Setting > Stacking > Stacking Status > Slot number

LABEL	DESCRIPTION
Slot	This field displays the slot ID of the Switch.
Stacking	This field displays whether the Switch is active in the stacking system.
Role	This field displays whether the stacked Switch is a master or linecard Switch.
Force Master Mode	This field displays whether the Force Master Mode is enabled or disabled on this Switch. The **Active Force Master Mode** forces this Switch to become a master Switch. This Switch will have the highest priority over all other Switch in the stack. If two Switches are set as masters, they will have the same priority level, but the Switch that has the longest active run-time will be selected as the master Switch automatically.
Priority	This field displays the priority level of the Switch. A higher number represents higher priority.
Slot ID After Reboot	This field displays the slot ID of the Switch after a reboot. You can save the slot ID of the Switch after a reboot by clicking **Freeze** in the **Stacking Configuration** screen. See Section 6.10.3 on page 97.
Stacking Status	This field displays whether the stacked Switch is active or inactive in a stack. **Init** means the slot ID is initialized by the master Switch.
Master Capable	This field displays whether the Switch has capacity to become a master Switch. **Auto** means the stack system master election process will determine if the Switch can be assigned as a master Switch.
Stacking MAC Address	This field displays the stacking Switch MAC address.
Stacking Channel 1	This field displays the status of the port stacking channel 1 of the Switch. It will display up for active or down for inactive.
Stacking Channel 2	This field displays the status of the port stacking channel 2 of the Switch. It will display up for active or down for inactive.
Stacking Up Time	This field displays the time that the active Switch in a stack has been running.
ZyNOS version * Running/Flash	This field displays the ZyNOS firmware that is currently running on the Switch.

6.10.3 Stacking Configuration

A supported Switch can change between stacking and standalone mode by selecting the **Active** check box in the **Basic Setting** > **Stacking** > **Configuration** screen.

Note: When you change modes, all configurations except user accounts, but including running configuration, config01 and config02 will be erased and the Switch will reboot with a new config01. Therefore, you should back up previous configurations if you want to reload them later.

Stacking will automatically choose a master Switch in a stack but you can overwrite that by actively forcing a Switch to become a master Switch. In the **Stacking Configuration** screen, click **Active Force Master Mode** to choose the master Switch. This master Switch will have the highest priority over all other stacked Switches even when they have same priority value.

If two or more Switches have **Active Force Master Mode** enabled, then the Switch will use **System Priority** to determine which is master. If they have the same **System Priority**, then the Switch with the longest up-time is selected. Uptime is measured in increments of 10 minutes. The Switch with the higher number of increments is selected. If they have the same uptime, then the Switch with the lowest MAC address will be the master.

This is the master election priority in a stack system:

1 **Active Force Master Mode**

2 Highest **Stacking Priority**

3 Longest **System Up Time**

4 Lowest MAC Address

Note: Master election occurs when a stacking port link status changes (up / down). The link status changes when (for example):

- a stacking port cable is disconnected

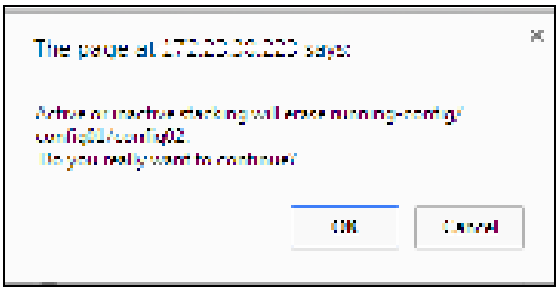
- a Switch in the stack reboots (as happens after you change stacking mode to standalone)

- you add a Switch to the stack or

- a Switch in the stack shuts down.

Use the following procedure to create a stack:

1 Select a Switch to be the master. Change its mode to stacking mode. You will see a message asking you to confirm the change. Click **OK** to confirm and the Switch will reboot automatically using a new config01.



2 After reboot completes, the master LED will turn on.

3 Configure the Switch stacking priority to a high value, such as 63.

4 Change a second Switch to stacking mode and wait for it to finish rebooting automatically. This master LED will also turn on.

5 Connect the two Switches using the stacking ports for the Switch defined.

6 The second Switch master LED will then turn off, and its **Sys** LED will blink while it's initializing. Please wait until it stops blinking, indicating that it has joined the stack.

7 Repeat steps 4 to 6 to connect other Switches to the stack.

When the Switch is in Stacking mode, the web configurator will change port and VLAN port settings to support the stacking mode. See Section 6.6 on page 69 and Section 7.7 on page 106 for details on the port settings.

Click **Basic Setting** > **Stacking** > **Configuration** to see the following screen.

Figure 59 Basic Setting > Stacking > Configuration

The following table describes the labels in this screen.

Table 38 Basic Setting > Stacking > Configuration

LABEL	DESCRIPTION
Active	Select the **Active** check box to put the Switch in stacking mode. This will erase the running configuration, config01 and config02. The master Switch's login will remain unchanged. If you want to reload a previous configuration, please back one up first.
Apply	Click **Apply** to activate the stacking mode.
Cancel	Click **Cancel** to clear the Active check box.
Force Master Mode	Select the **Force Master Mode** check box to force this Switch to become a master Switch.
System Priority	Enter a number (from1 to 63) to assign a priority for the stacking Switch. The higher the number, the higher the priority.
Apply	Click **Apply** to save the **Active Force Master Mode** and **System Priority** fields.
Cancel	Click **Cancel** to clear the **Active Force Master Mode** and **System Priority** fields.
Slot ID Freeze	Click the **Freeze** button to have the Switch retain its slot ID after reboot.
Slot	This field displays the slot or port channel of the stacked Switch.
MAC Address	This field displays the MAC address of the stacked Switch.
Type	This field displays the model name of the Switch.
Slot ID After Reboot	Choose **Auto** to have a new slot ID assigned after reboot. If you want to keep the original slot ID after reboot, you can click **Freeze** or select an ID in the **Slot ID After Reboot** list box.
Apply	Click **Apply** to save the Slot ID After reboot field.
Cancel	Click **Cancel** to clear the Slot ID After reboot field.

6.11 DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Use the **DNS** screen to configure and view the default DNS servers on the Switch.

Figure 60 Basic Setting > DNS

The following table describes the labels in this screen.

Table 39 Basic Setting > DNS

LABEL	DESCRIPTION
Static Domain Name Server	
Preference	This is the priority of the DNS server address.

Table 39 Basic Setting > DNS (continued)

LABEL	DESCRIPTION
Server Address	Enter a domain name server IPv6/IPv4 address in order to be able to use a domain name instead of an IP address.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Domain Name Server Table	
Index	This field displays priority of the DNS server address.
Server Address	This field displays the IP address of the DNS server.
Source	This field displays whether the DNS server address is configured manually (**Static**) or obtained automatically using DHCP/DHCPv6 (**Dynamic**).

7

VLAN

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen which is only available in standalone mode. The Switch does not support port-based VLANs in stacking mode. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

7.1 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 for the TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes for the TCI (Tag Control Information, starting 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 the value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4,094.

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

7.1.1 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.

7.2 Automatic VLAN Registration

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

7.2.1 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.

7.2.1.1 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.

7.2.2 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 40 IEEE 802.1Q VLAN Terminology

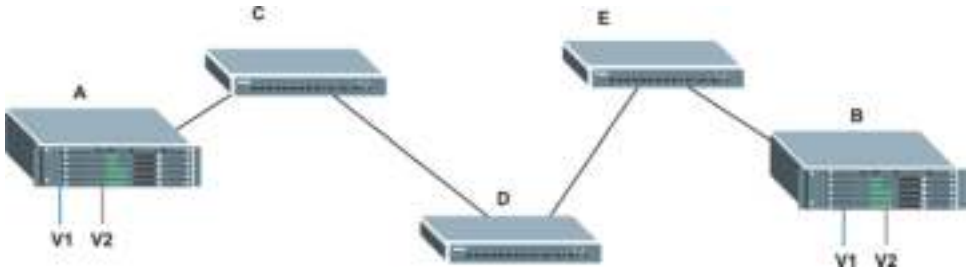
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/ deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	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.
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.

7.3 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.

The following figure describes **VLAN Trunking**. 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).

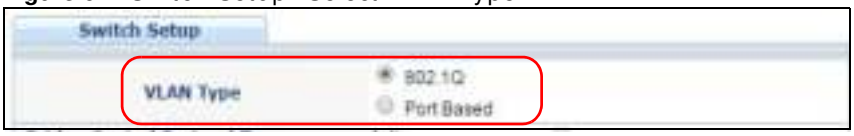
Figure 61 Port VLAN Trunking



7.4 Select the VLAN Type

Select a VLAN type in the **Basic Setting > Switch Setup** screen. VLAN Type is not applicable in Stacking mode.

Figure 62 Switch Setup: Select VLAN Type



7.5 802.1Q Static VLAN

Make sure **802.1Q** is selected in the **Basic Setting > Switch Setup** screen.

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

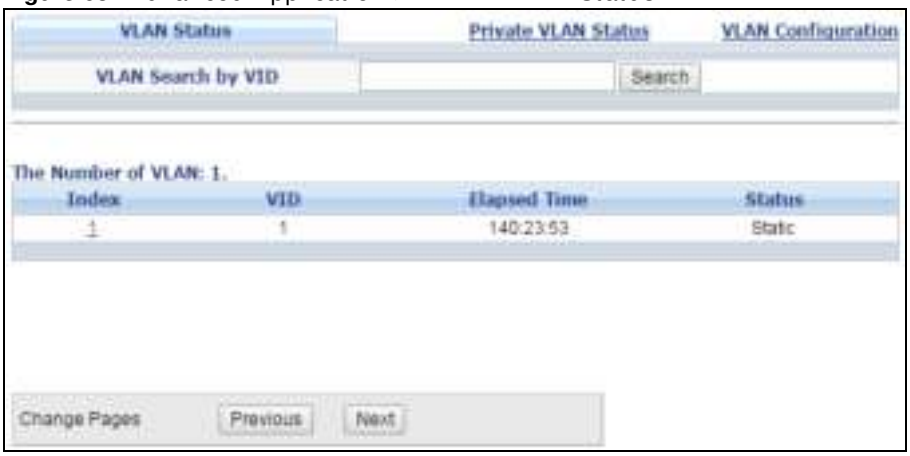
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

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

7.5.1 VLAN Status

See Section 7.1 on page 101 for more information on 802.1Q VLAN. Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 63 Advanced Application > VLAN: VLAN Status



The following table describes the labels in this screen.

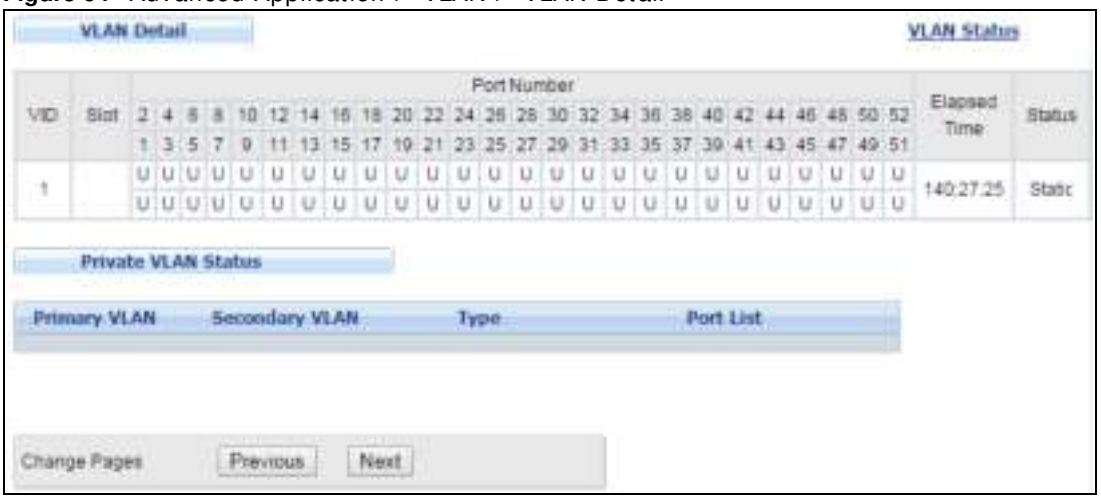
Table 41 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click **Search** to display only the specified VLAN(s) in the list below. Leave this field blank and click **Search** to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the **Search** button to look for certain VLANs.
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 **Static VLAN** screen.
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. • **Dynamic** - using GVRP • **Static** - manually added as a normal VLAN • **Private** - manually added as a private VLAN (primary, isolated or community) • **Voice** - manually added as a Voice VLAN • **RMirror** - manually added as a remote port mirroring VLAN • **MVR** - added via Multicast VLAN Registration (MVR)
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

7.5.2 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See Section 7.1 on page 101 for more information on 802.1Q VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 64 Advanced Application > VLAN > VLAN Detail



The following table describes the labels in this screen.

Table 42 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Slot	'Slot' refers to a Switch in the the 'virtual chassis' stack. This field displays the slot ID of the stacked Switch.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** 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. • **Dynamic** - using GVRP • **Static** - manually added as a normal VLAN • **Private** - manually added as a private VLAN (primary, isolated or community) • **Voice** - manually added as a Voice VLAN • **RMirror** - manually added as a remote port mirroring VLAN • **MVR** - added via Multicast VLAN Registration (MVR)
Private VLAN Status	These fields show private VLAN information for the selected VLAN. See Section 33.1 on page 336 for more information on private VLANs.
Primary VLAN	This field shows the primary VLAN ID in the selected VLAN.
Secondary VLAN	This field shows the secondary VLAN ID in the selected VLAN.
Type	This field shows the type of private VLAN: **Primary**, **Community** or **Isolated**.

Table 42 Advanced Application > VLAN > VLAN Detail (continued)

LABEL	DESCRIPTION
Port List	This shows the ports mapped to the private VLAN using the **Advanced Application > Private VLAN** or **Advanced Application > VLAN > Static VLAN** screen.
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

7.6 Private VLAN Status

Use this screen to view all private VLANs created on the Switch. Click **Advanced Application** > **VLAN** > **Private VLAN Status** to see the following screen.

Figure 65 Advanced Application > VLAN > Private VLAN Status

The following table describes the labels in this screen.

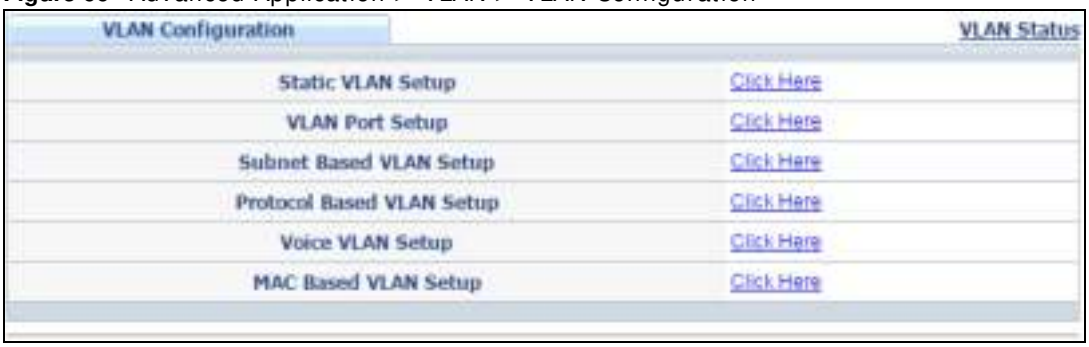
Table 43 Advanced Application > VLAN > Private VLAN Status

LABEL	DESCRIPTION
Private VLAN Status	These fields show information for the all private VLANs. See also **Advanced Application > Private VLAN**.
Primary VLAN	This field shows the primary VLAN ID in a private VLAN.
Secondary VLAN	This field shows the secondary VLAN ID in a private VLAN.
Type	This field shows the type of private VLAN: **Primary**, **Community** or **Isolated**.
Port List	This shows the ports mapped to the private VLAN using the **Advanced Application > Private VLAN** or **Advanced Application > VLAN > Static VLAN** screen.
Change Pages	Use the **Previous** and **Next** buttons to display different pages.

7.7 VLAN Configuration

Use this screen to view IEEE 802.1Q VLAN parameters for the Switch. Click **Advanced Application** > **VLAN** > **VLAN Configuration** to see the following screen.

Figure 66 Advanced Application > VLAN > VLAN Configuration



The following table describes the labels in the above screen.

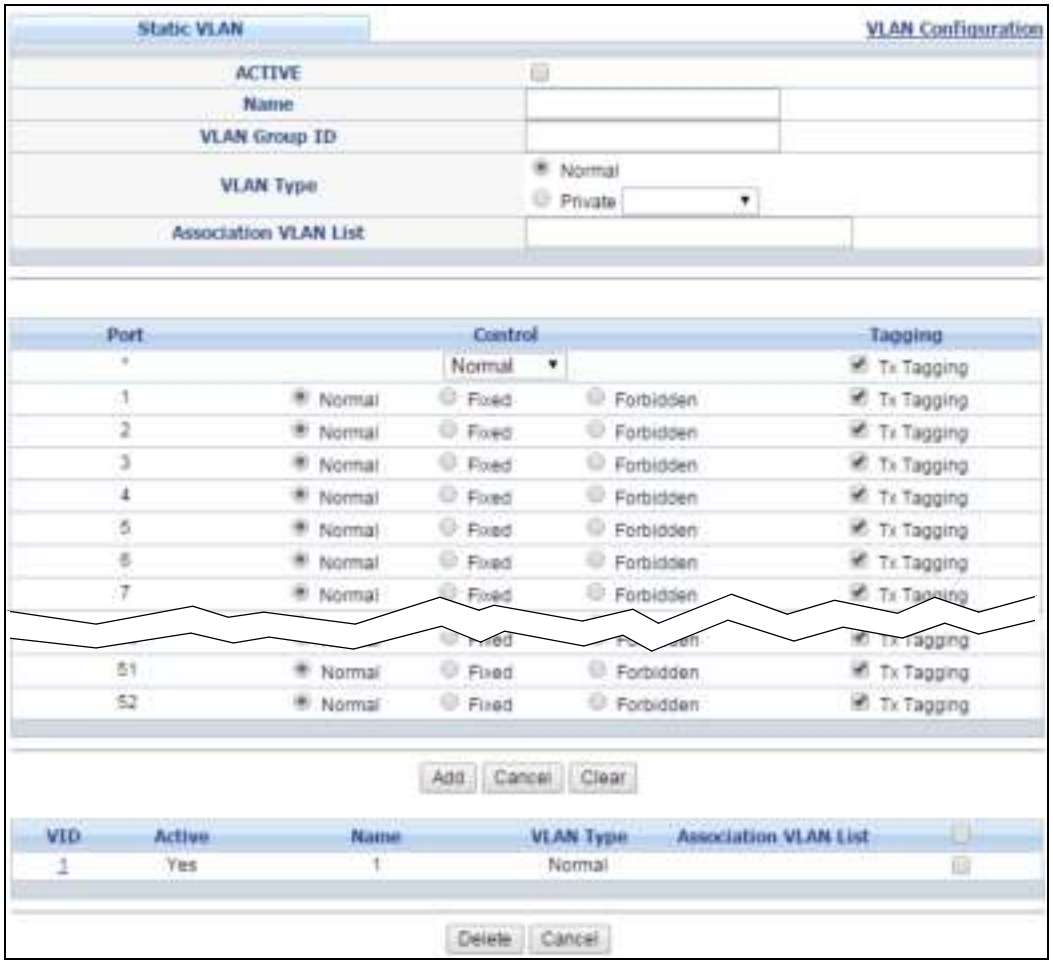
Table 44 Advanced Application > VLAN > VLAN Configuration

LABEL	DESCRIPTION
Static VLAN Setup	Click **Click Here** to configure the Static VLAN for the Switch.
VLAN Port Setup	Click **Click Here** to configure the VLAN Port for the Switch.
Subnet Based VLAN Setup	Click **Click Here** to configure the Subnet Based VLAN for the Switch.
Protocol Based VLAN Setup	Click **Click Here** to configure the Protocol Based VLAN for the Switch.
Voice VLAN Setup	Click **Click Here** to configure the Voice VLAN for the Switch.
MAC Based VLAN Setup	Click **Click Here** to configure the MAC Based VLAN for the Switch.

7.7.1 Configure a Static VLAN

Use this screen to configure a static VLAN for the Switch. Click the **Static VLAN Setup** link in the **VLAN Configuration** screen to display the screen as shown next.

Figure 67 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup



The following table describes the related labels in this screen.

Table 45 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

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; spaces are allowed.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
VLAN Type	Select **Normal** (static) or **Private**. For **Private** VLANs, select **Primary**, **Isolated** or **Community**.
Association VLAN List	**Primary** private VLANs can associate with several (secondary) **Community** private VLANs and up to one (secondary) **Isolated** private VLAN. You only configure **VLAN Association List** for **Primary** private VLANs. Use a dash to associate consecutive VLANs and a comma (no spaces) to associate non-consecutive VLANs. For example, 51-53 includes 51, 52 and 53, but 51,53 does not include 52. Secondary private VLANs can only be associated with one primary private VLAN.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.

Table 45 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup (continued)

LABEL	DESCRIPTION
Port	The port number identifies the port you are configuring. In stacking mode, the first number represents the slot and the second 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.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
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 (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
VLAN Type	This field displays the **Normal** or **Private** (**Primary**, **Isolated** or **Community**) type VLAN configured in the top part of this screen.
Association VLAN List	This field displays which secondary private VLANs are associated with a primary private VLAN configured in the top part of this screen.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

7.7.2 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See Section 7.1 on page 101 for more information on 802.1Q VLAN. Click the **VLAN Port Setup** link in the **VLAN Configuration** screen.

Figure 68 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup: Standalone mode

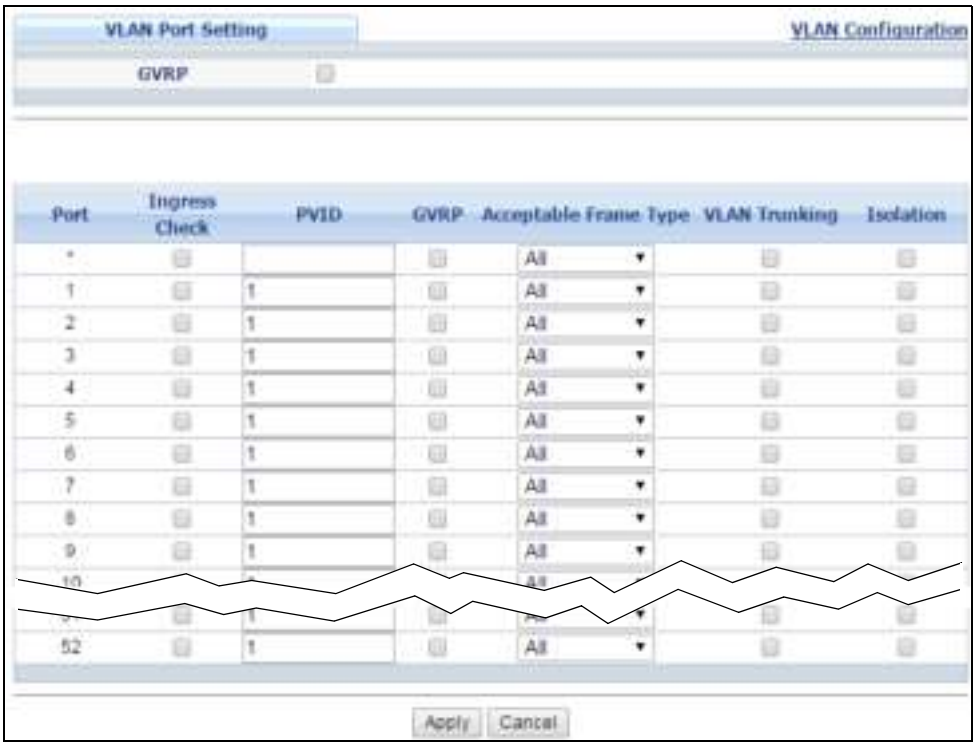
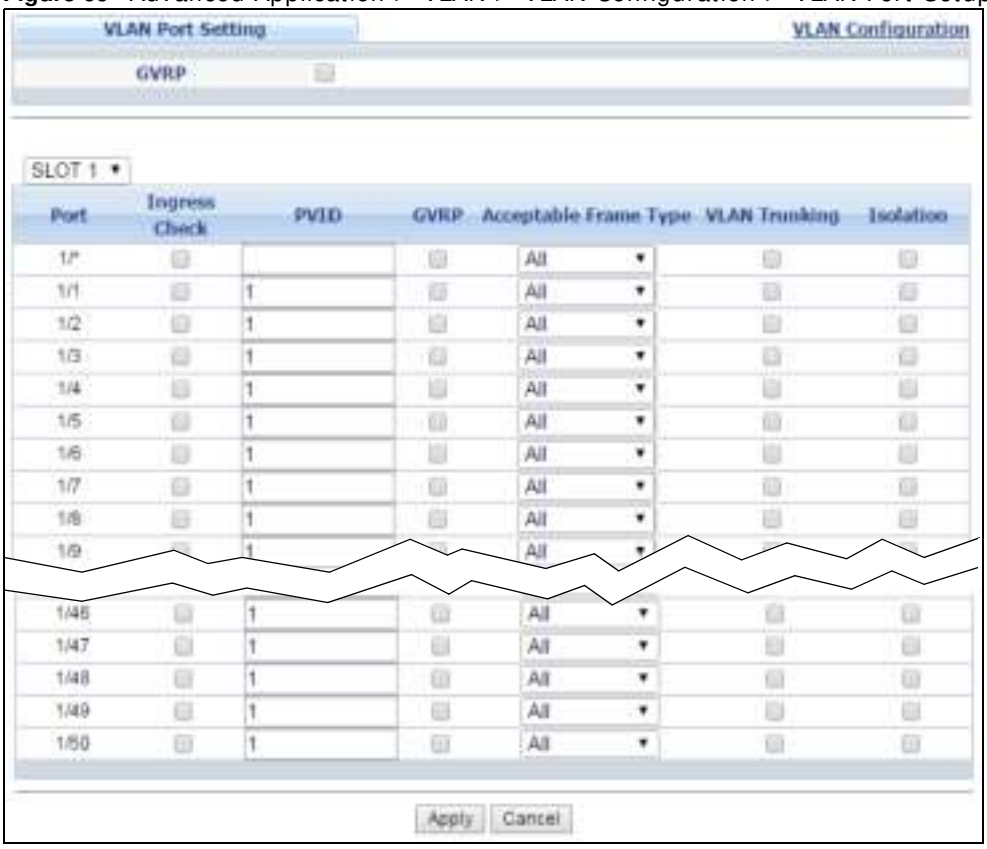


Figure 69 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup: Stacking mode



The following table describes the labels in this screen.

Table 46 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup: Standalone/ Stacking mode

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.
SLOT1	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch.
Port	This field displays the port number of the Switch. In stacking mode, the first number represents the slot and the second the port number. Please note that the default stacking ports (the last two ports of your Switch) cannot be configured. They are reserved for stacking only.
*	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 PVID (Port VLAN ID) is a tag that 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.
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 **All**, **Tag Only** and **Untag Only**. Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped. Select **Untag Only** to accept only untagged frames on this port. All tagged frames will be dropped. Note that when the Switch is in stacking mode and the master Switch has VLAN1, all other ports will be configured to untagged port.
VLAN Trunking	Enable **VLAN Trunking** 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.
Isolation	Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is not enabled.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.7.3 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

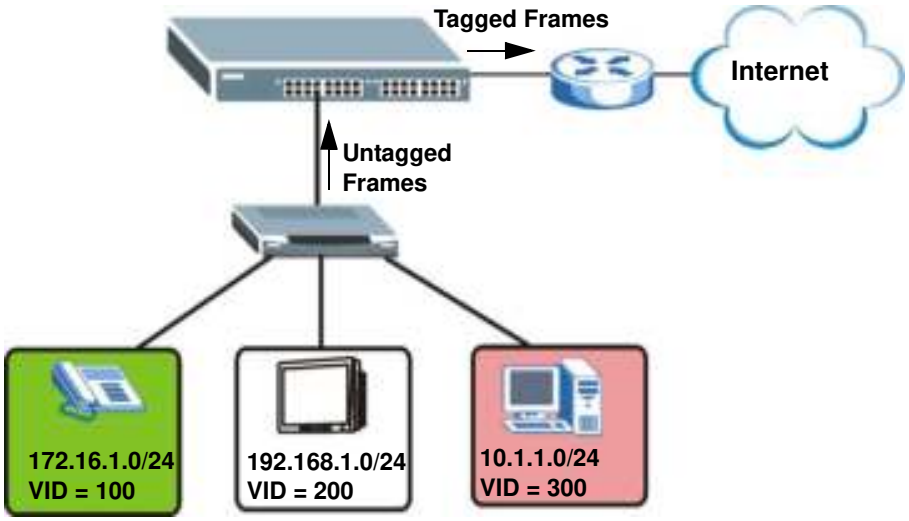
subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

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

For example, an ISP (Internet Service 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 can then 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 can 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 can 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.

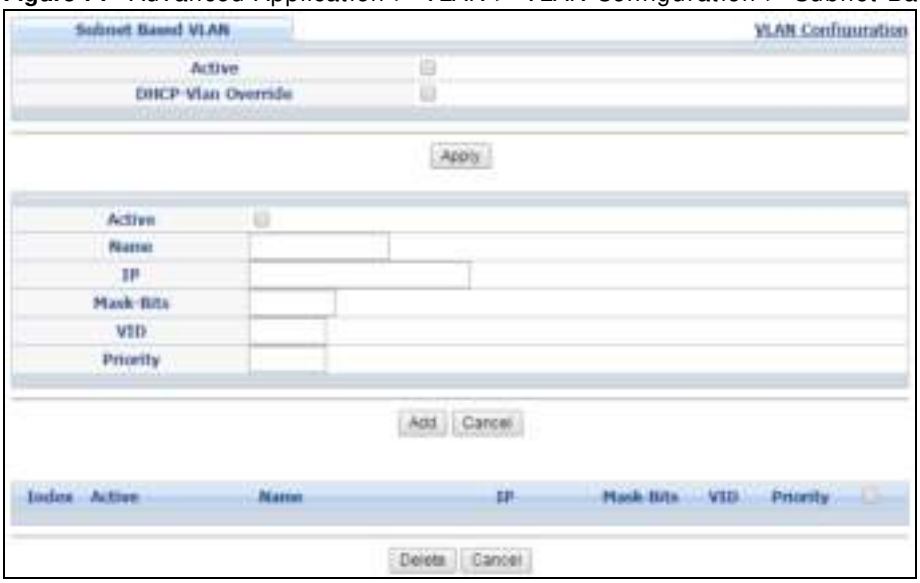
Figure 70 Subnet Based VLAN Application Example



7.7.3.1 Configuring Subnet Based VLAN

Click the **Subnet Based VLAN Setup** link in the **VLAN Configuration** screen to display the configuration screen as shown.

Figure 71 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup



The following table describes the labels in this screen.

Table 47 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Select this check 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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Select this check box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alphanumeric characters to identify this subnet based VLAN.
IP	Enter the IP 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 **Advanced Application > VLAN > Static VLAN** screen.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
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.

Table 47 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup

LABEL	DESCRIPTION
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.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click **Cancel** to clear the check boxes.

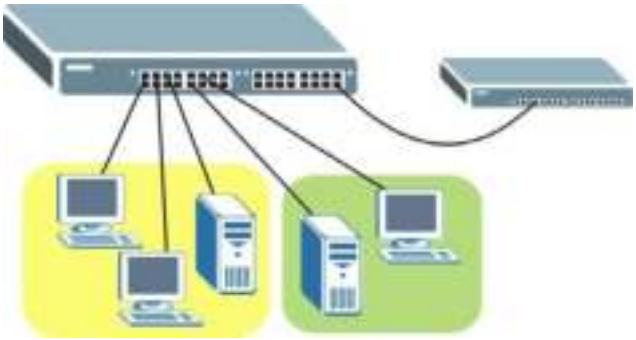
7.7.4 Protocol Based VLANs

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, ports 1, 2, 3 and 4 belong to static VLAN 100, and ports 4, 5, 6, 7 belong to static VLAN 120. You can configure a protocol based VLAN A with priority 2 for ARP traffic received on port 1, 2 and 3. You can also have a protocol based VLAN B with priority 3 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.

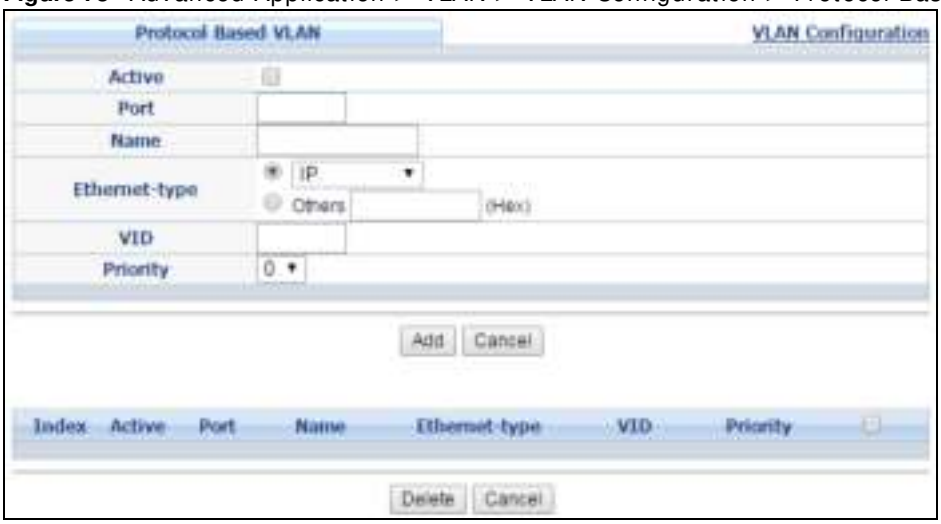
Figure 72 Protocol Based VLAN Application Example



7.7.4.1 Configuring Protocol Based VLAN

Click the **Protocol Based VLAN Setup** link in the **VLAN Configuration** screen to display the configuration screen as shown.

Figure 73 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup



The following table describes the labels in this screen.

Table 48 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Select this check box to activate this protocol based VLAN.
Port	Type a port number to be included in this protocol based VLAN. In stacking mode, the first box field is the slot ID and the second field is the port number. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 7 on page 101 for more details on setting up VLANs.
Name	Enter up to 32 alphanumeric 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 **Others** 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 **Advanced Application > VLAN > Static VLAN** screen.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
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. In stacking mode, the first number represents the slot and the second the port number.
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.

Table 48 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click **Cancel** to clear the check boxes.

7.7.4.2 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 using the screen below:

1 Activate this protocol based VLAN.

2 Type the port number you want to include in this protocol based VLAN. Type **1**.

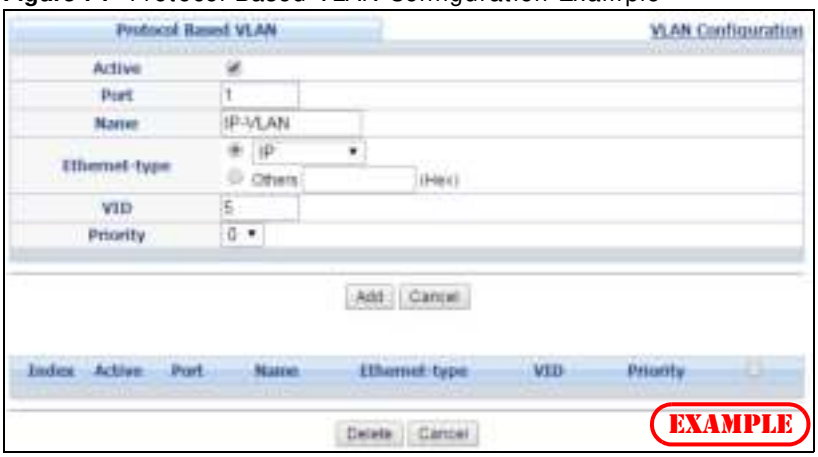
3 Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.

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 74 Protocol Based VLAN Configuration Example



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**.

7.8 Port-based VLAN Setup (Standalone Mode)

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.

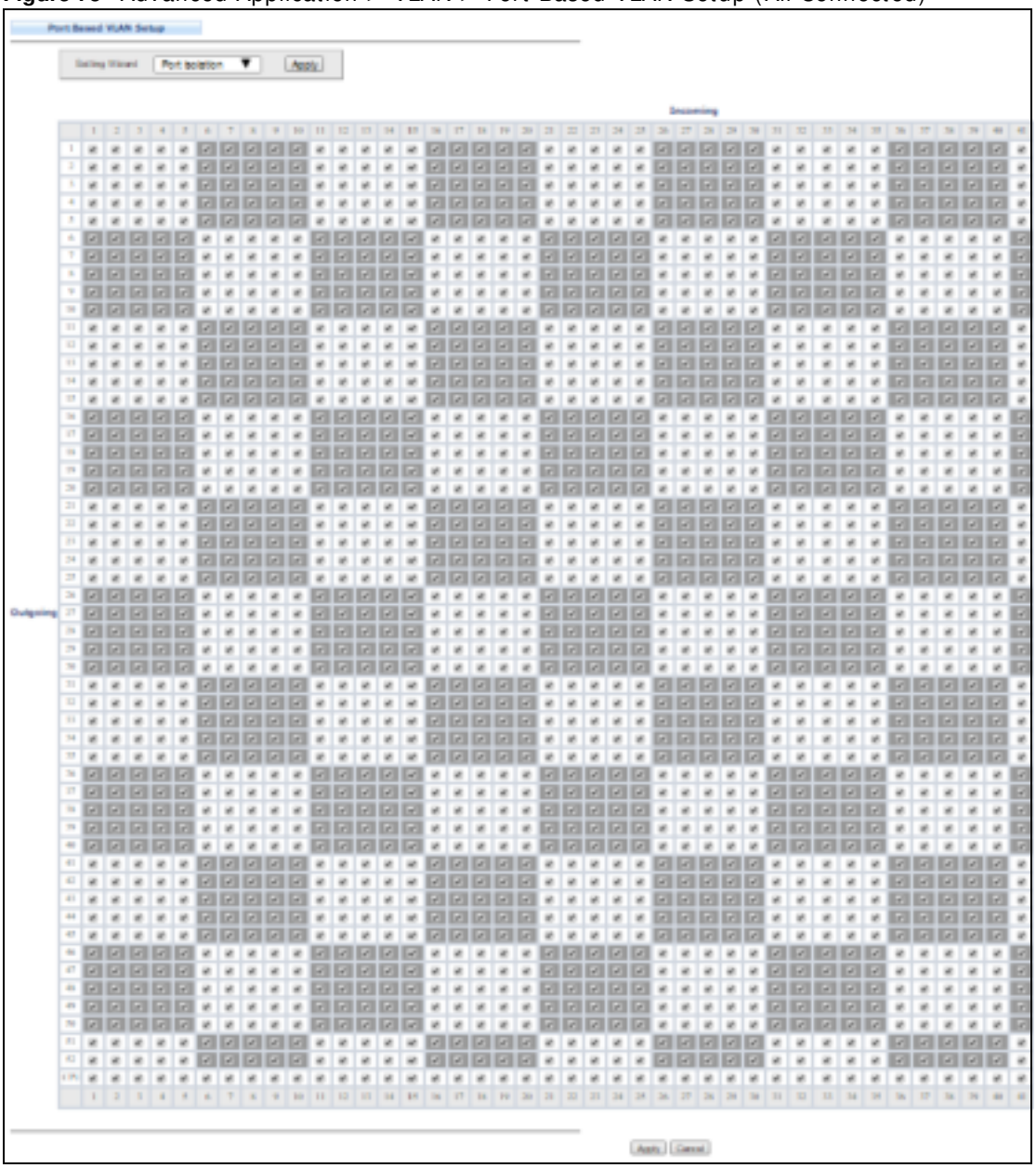
The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

7.8.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen and then click **VLAN** from the navigation panel to display the following screen. Select either **All Connected** or **Port Isolated** from the drop-down list depending on your VLAN and VLAN security requirements. If VLAN members need to communicate directly with each other, then select **All Connected**. Select **Port Isolated** if you want to restrict users from communicating directly. Click **Apply** to save your settings.

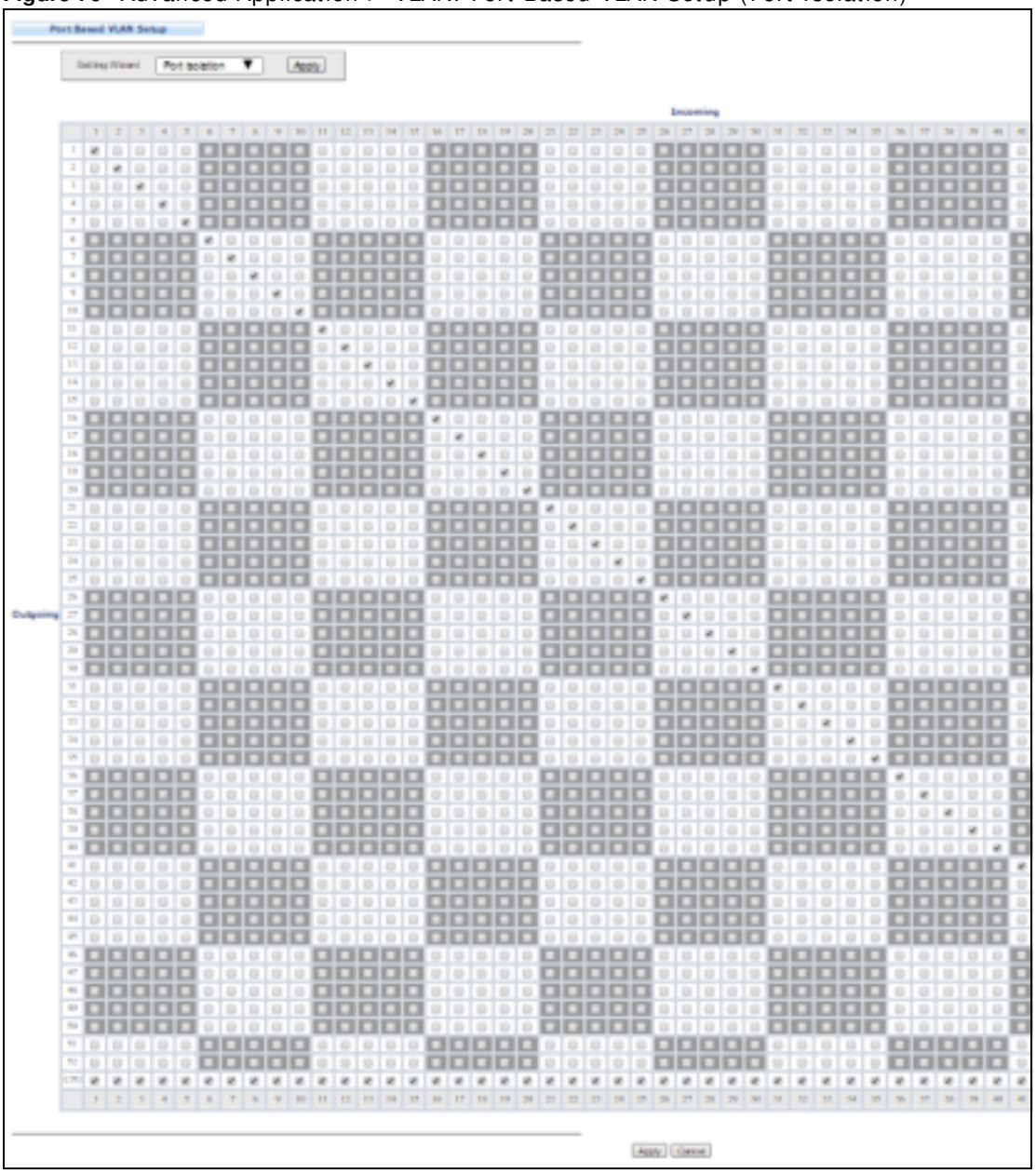
The following screen shows users on a port-based, all-connected VLAN configuration.

Figure 75 Advanced Application > VLAN > Port Based VLAN Setup (All Connected)



The following screen shows users on a port-based, port-isolated VLAN configuration.

Figure 76 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 49 Advanced Application > VLAN: Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose **All connected** or **Port isolation**. **All connected** 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. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. After you make your selection, click **Apply** (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 **Apply** at the bottom of the screen.
Incoming	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). **CPU** 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.
Outgoing	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. **CPU** 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.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.9 Voice VLAN

Voice VLAN ensures that the sound quality of an IP phone is preserved from deteriorating when the data traffic on the Switch ports is high. It groups the voice traffic with defined priority into an assigned VLAN which enables the separation of voice and data traffic coming onto the Switch port.

You can set priority level to the Voice VLAN and add MAC address of IP phones from specific manufacturers by using its ID from the Organizationally Unique Identifiers (OUI).

Click the **Voice VLAN Setup** link in the **VLAN Configuration** screen to display the configuration screen as shown.

Figure 77 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

The following table describes the fields in the above screen.

Table 50 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
Voice VLAN Global Setup	
Voice VLAN	Click the Voice VLAN radio button if you want to enable the Voice VLAN feature. Type a VLAN ID number in the box next to the radio button that is associated with the Voice VLAN. Click **Disable** radio button if you do not want to enable the Voice VLAN feature.
Priority	Select the priority level of the Voice VLAN from 0 to 7. Default setting is 5.The higher the numeric value you assign, the higher the priority for this Voice VLAN.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to default settings.
Voice VLAN OUI Setup	
OUI address	Type the IP Phone manufacturer's OUI MAC address. The first three byes is the manufacturer identifier, the last three bytes is a unique station ID.
OUI mask	Type the IP Phone manufacturer's OUI mask address.
Description	Type an description up to 32 characters for the Voice VLAN device. For example: Siemens.
Add	Click **Add** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This field displays the index number of the Voice VLAN.
OUI address	This field displays the OUI address of the Voice VLAN.
OUI mask	This field displays the OUI mask address of the Voice VLAN.
Description	This field displays the description of the Voice VLAN with OUI address.

Table 50 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

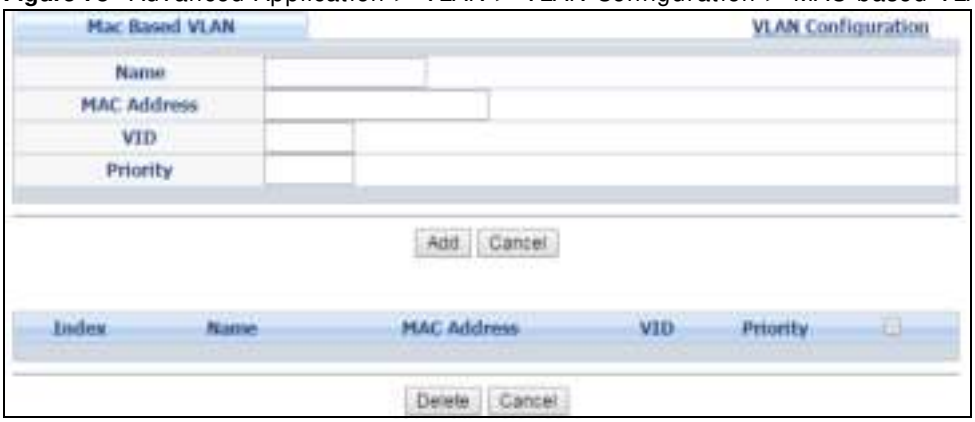
7.10 MAC Based VLAN

The MAC-based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. When untagged packets arrive at the switch, the source MAC address of the packet is looked up in a MAC to VLAN mapping table. If an entry is found, the corresponding VLAN ID is assigned to the packet. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped.

This feature allows users to change ports without having to reconfigure the VLAN. You can assign priority to the MAC-based VLAN and define a MAC to VLAN mapping table by entering a specified source MAC address in the MAC-based VLAN setup screen. You can also delete a MAC-based VLAN entry in the same screen.

Click the **MAC-based VLAN Setup** link in the **VLAN Configuration** screen to see the following screen.

Figure 78 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup



The following table describes the fields in the above screen.

Table 51 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup

LABEL	DESCRIPTION
Name	Type a name up to 32 alpha numeric characters for the MAC-based VLAN entry.
MAC Address	Type a MAC address that is bind to the MAC-based VLAN entry. This is the source MAC address of the data packet that is looked up when untagged packets arrive at the Switch.
VID	Type an ID (from 1 to 4094) for the VLAN ID that is associated with the MAC-based VLAN entry.

Table 51 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup

LABEL	DESCRIPTION
Priority	Type a priority (0-7) for the MAC-based VLAN entry.The higher the numeric value you assign, the higher the priority for this MAC-based VLAN entry.
Add	Click **Add** to save the new MAC-based VLAN entry.
Cancel	Click **Cancel** to clear the fields in the MAC-based VLAN entry.
Index	This field displays the index number of the MAC-based VLAN entry.
Name	This field displays the name of the MAC-based VLAN entry.
MAC Address	This field displays the source MAC address that is bind to the MAC-based VLAN entry.
VID	This field displays the VLAN ID of the MAC-based VLAN entry.
Priority	This field displays the priority level of the MAC-based VLAN entry.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

8

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

8.1 Overview

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

8.2 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 allows only computers in the MAC address table on a port to access the Switch. See Chapter 17 on page 195 for more information on port security.

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

Figure 79 Advanced Application > Static MAC Forwarding (Standalone mode)

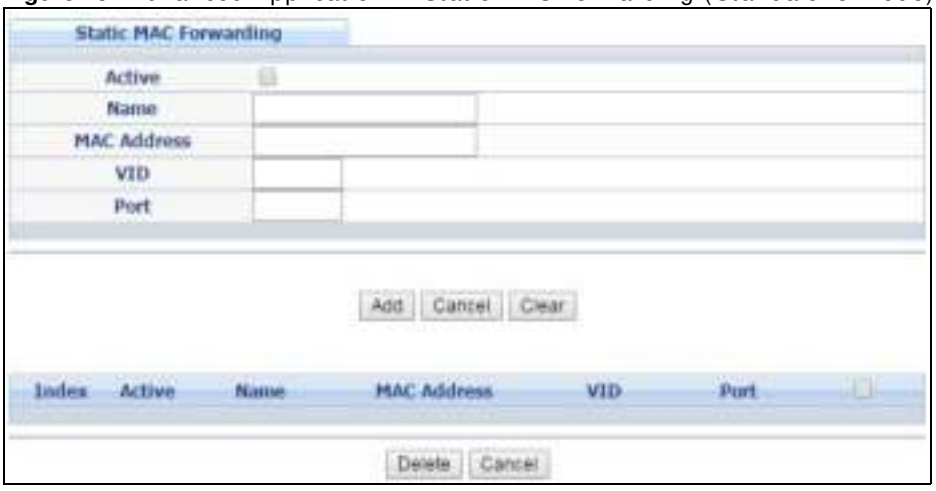
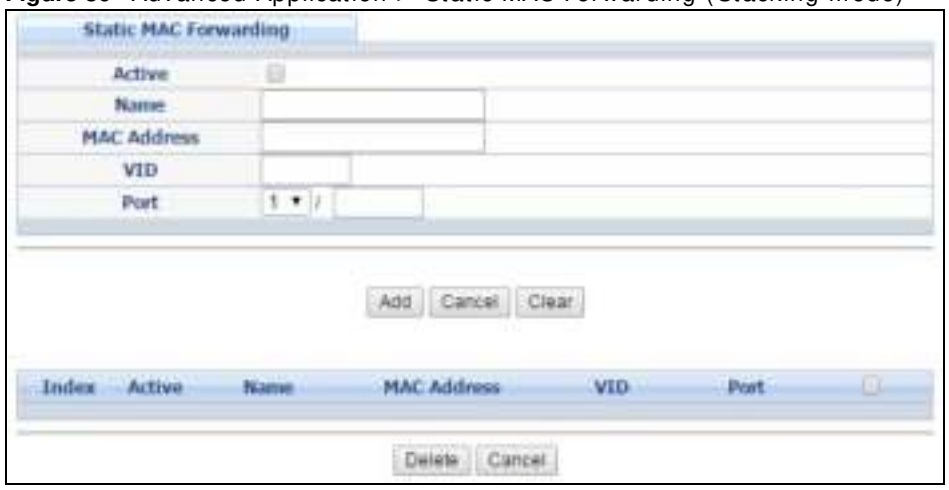


Figure 80 Advanced Application > Static MAC Forwarding (Stacking mode)



The following table describes the labels in this screen.

Table 52 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. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port(standalone or stacking mode)	Enter the port where the MAC address entered in the previous field will be automatically forwarded. In stacking mode, the first box field is the slot ID and the second field is the port number.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
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 (**Yes**) or not (**No**). 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. In stacking mode, the first number represents the slot and the second the port number.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.

Table 52 Advanced Application > Static MAC Forwarding (continued)

LABEL	DESCRIPTION
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

9

Static Multicast Forward Setup

Use these screens to configure static multicast address forwarding.

9.1 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 > IPv4 Multicast > IGMP Snooping** screen (see Section 23.3.1 on page 230). Figure 81 shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. Figure 82 shows frames being forwarded to devices connected to port 3. Figure 83 shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 81 No Static Multicast Forwarding

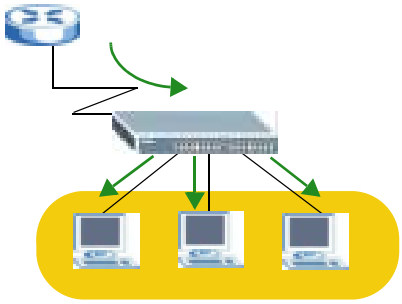


Figure 82 Static Multicast Forwarding to A Single Port

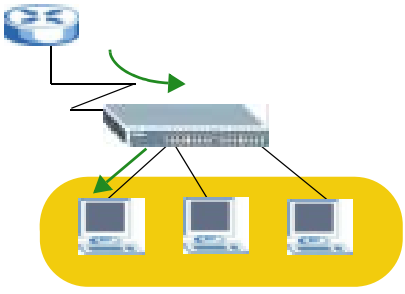
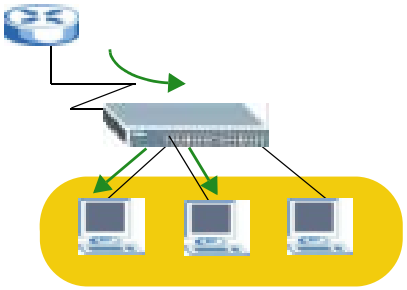


Figure 83 Static Multicast Forwarding to Multiple Ports

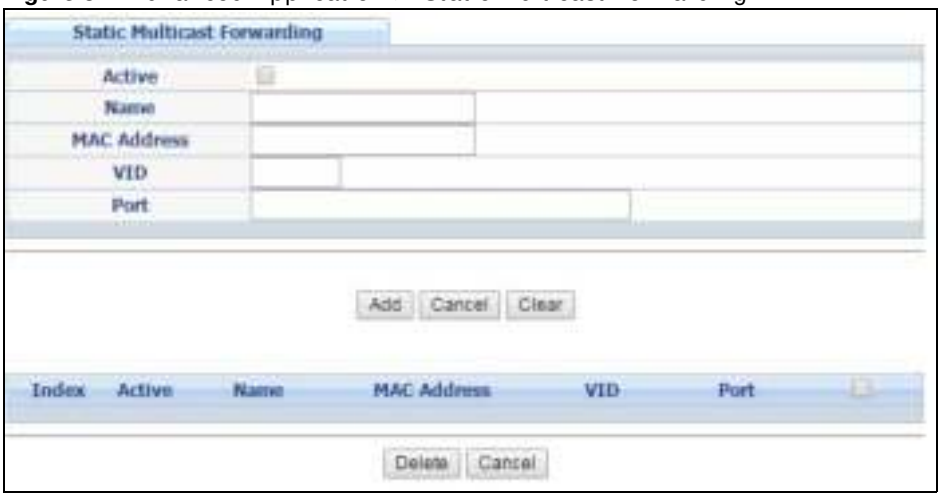


9.2 Configuring Static Multicast Forwarding

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 84 Advanced Application > Static Multicast Forwarding



The following table describes the labels in this screen.

Table 53 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.

Table 53 Advanced Application > Static Multicast Forwarding (continued)

LABEL	DESCRIPTION
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 a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to reset the fields to the factory defaults.
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 (**Yes**) or not (**No**). 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.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

10

Filtering

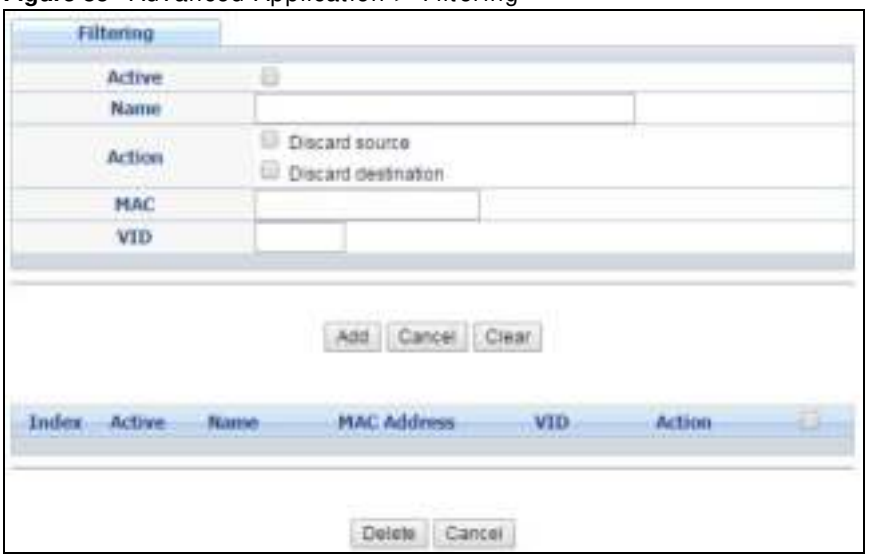
This chapter discusses MAC address port filtering.

10.1 Configure a Filtering Rule

Configure the Switch to filter traffic based on the traffic's source, destination MAC addresses and/or VLAN group (ID).

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

Figure 85 Advanced Application > Filtering



The following table describes the related labels in this screen.

Table 54 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.

Table 54 Advanced Application > FIltering (continued)

LABEL	DESCRIPTION
Action	Select **Discard source** to drop frames from the source MAC address (specified in the **MAC** field). The Switch can still send frames to the MAC address. Select **Discard destination** to drop frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to/from the MAC address specified in the **MAC** field.
MAC	Type a MAC address in a valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset 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 **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purposes 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 **Discard source**, **Discard destination**, or **Discard both** depending on what you configured above.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rule(s) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

11

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.

11.1 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 and then the root bridge 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.

11.1.1 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 55 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 55 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 bridge communicates with the root through the root port. The root port 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.

11.1.2 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.

11.1.3 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 56 STP Port States

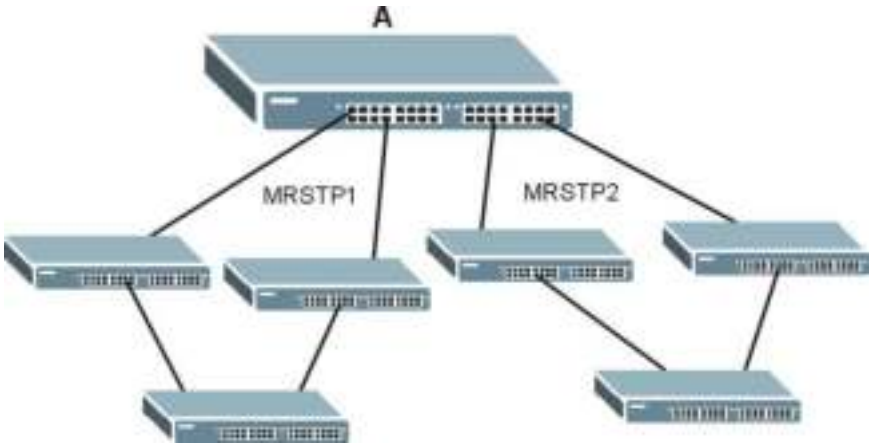
PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are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

11.1.4 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 (**MRSTP1** and **MRSTP2**) on switch **A**.

Figure 86 MRSTP Network Example



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.

11.1.5 Multiple STP

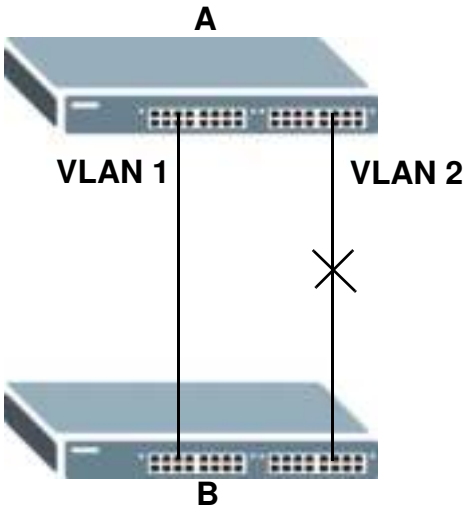
Multiple Spanning Tree Protocol (IEEE 802.1s) is backwards compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- 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.

11.1.5.1 MSTP Network Example

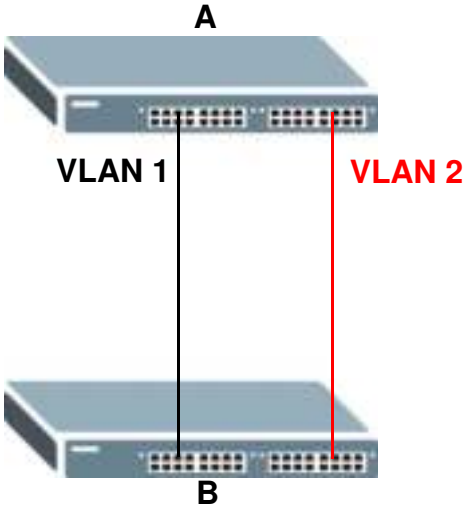
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 87 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 88 MSTP Network Example



11.1.5.2 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:

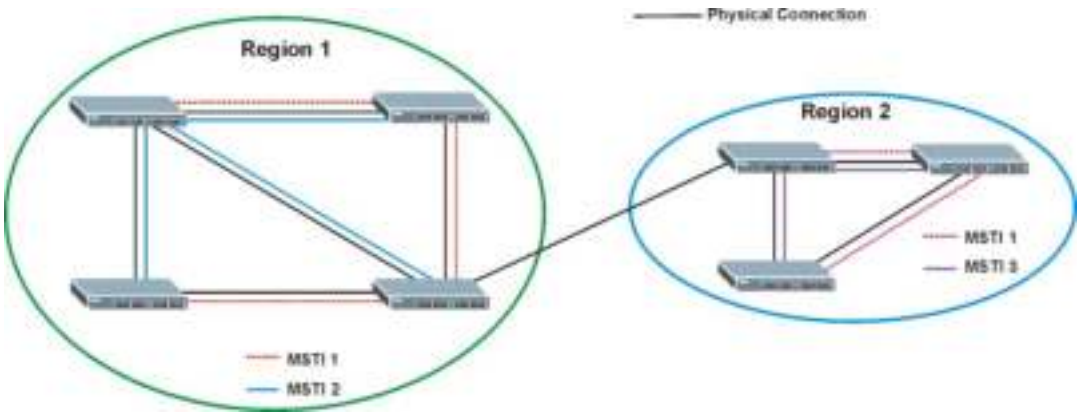
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

11.1.5.3 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.

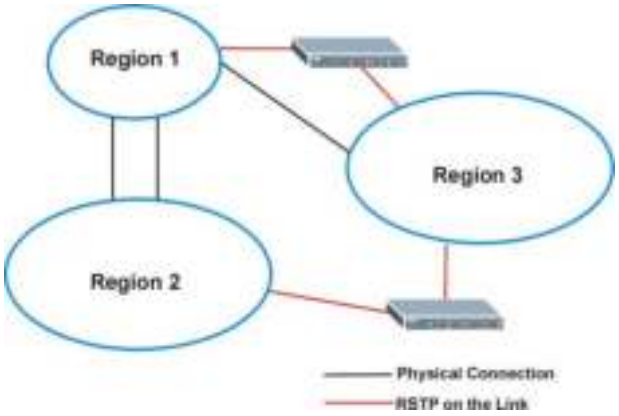
Figure 89 MSTIs in Different Regions



11.1.5.4 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 90 MSTP and Legacy RSTP Network Example



11.2 Spanning Tree Protocol Status Screen

Click **Advanced Application** > **Spanning Tree Protocol** to see the screen as shown.

Figure 91 Advanced Application > Spanning Tree Protocol (Standalone mode)

Figure 92 Advanced Application > Spanning Tree Protocol (Stacking mode)

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.

11.3 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 93 Advanced Application > Spanning Tree Protocol > Configuration

The following table describes the labels in this screen.

Table 57 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree**, **Multiple Rapid Spanning Tree** or **Multiple Spanning Tree**. See Section 11.1 on page 132 for background information on STP.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 11.1 on page 132 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 94 Advanced Application > Spanning Tree Protocol > RSTP (Standalone mode)

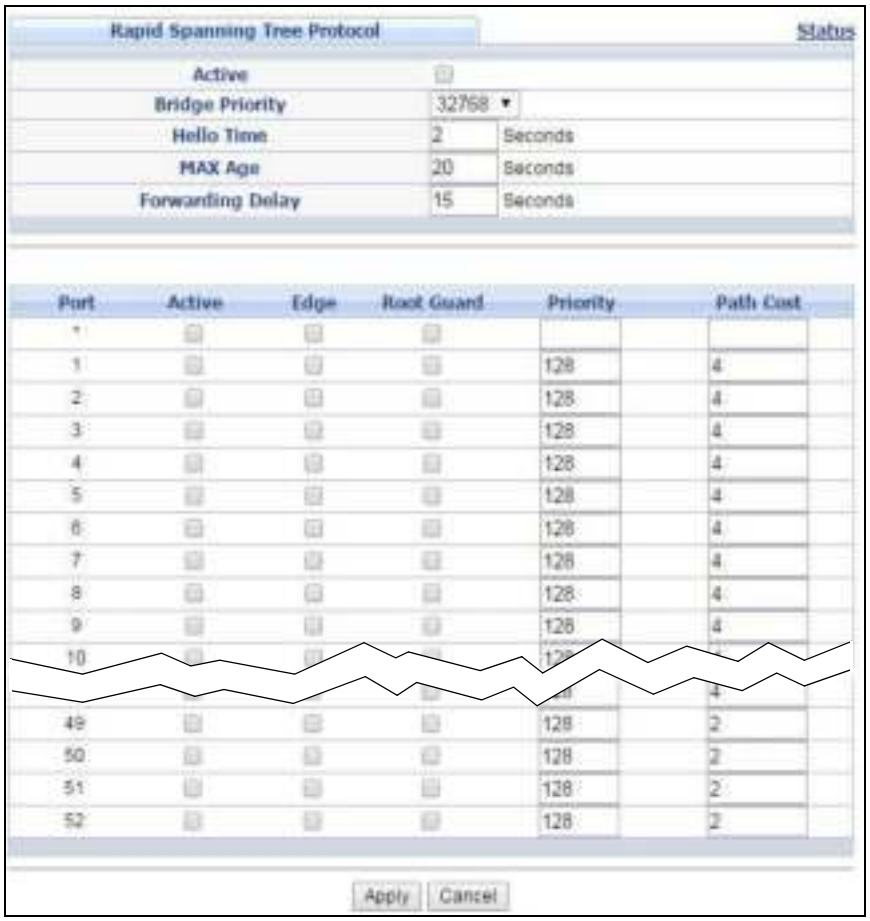
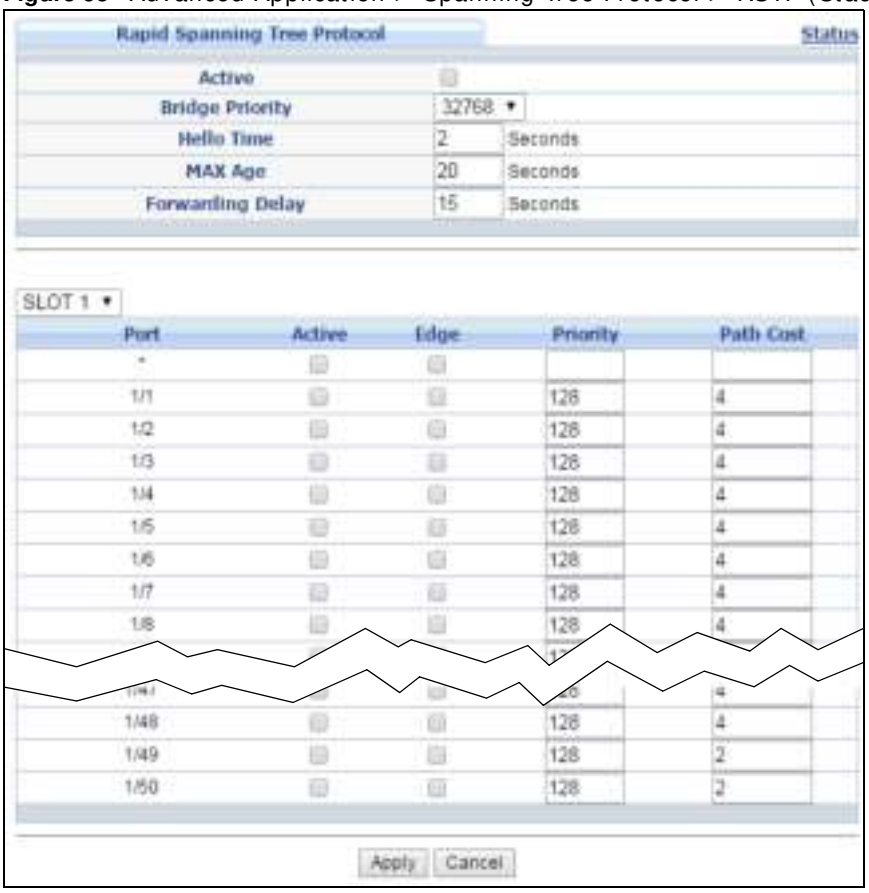


Figure 95 Advanced Application > Spanning Tree Protocol > RSTP (Stacking mode)



The following table describes the labels in this screen.

Table 58 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen (see Figure 96 on page 141).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP. Note: You must also activate **Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** 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.

Table 58 Advanced Application > Spanning Tree Protocol > RSTP (continued)

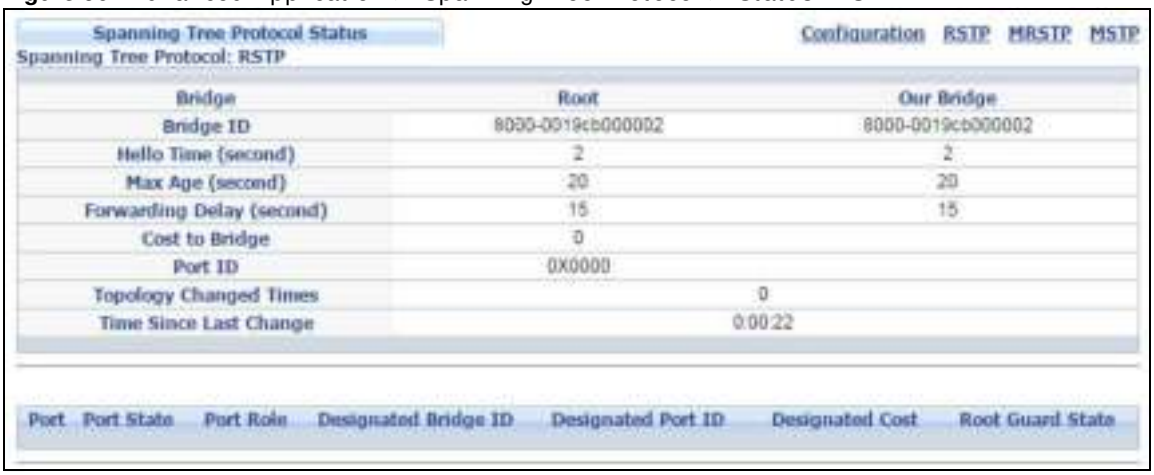
LABEL	DESCRIPTION
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes 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) a 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 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone and stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Root Guard (Standalone mode)	Select this check box to enable root guard on this port in order to prevent the switch(es) attached to the port from becoming the root bridge. With root guard enabled, a port is blocked when the Switch receives a superior BPDU on it. The Switch allows traffic to pass through this port again when the switch connected to the port stops to send superior BPDUs.
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 Table 55 on page 132 for more information.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.5 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 11.1 on page 132 for more information on RSTP.

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

Figure 96 Advanced Application > Spanning Tree Protocol > Status: RSTP



The following table describes the labels in this screen.

Table 59 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **RSTP** to edit RSTP settings on the Switch.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of the bridge priority plus the MAC address. This ID is the same for **Root** and **Our Bridge** 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) a 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). See Section 11.1.3 on page 133 for information on port states. Note: 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.
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.
Port	This field displays the number of the port on the Switch.

Table 59 Advanced Application > Spanning Tree Protocol > Status: RSTP (continued)

LABEL	DESCRIPTION
Port State	This field displays the port state in STP. • **Discarding** - The port does not forward/process received frames or learn MAC addresses, but still listens for BPDUs. • **Learning** - The port learns MAC addresses and processes BPDUs, but does not forward frames yet. • **Forwarding** - The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.
Port Role	This field displays the role of the port in STP. • **Root** - A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does not have a root port. • **Designated** - A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • **Alternate** - A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • **Backup** - A blocked port, which has a backup/redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • **Disabled** - Not strictly part of STP. The port can be disabled manually.
Designated Bridge ID	This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected.
Designated Port ID	This field displays the priority and number of the bridge port (on the designated bridge), through which the designated bridge transmits the stored configuration messages.
Designated Cost	This field displays the path cost to the LAN segment to which the port is connected when the port is a designated port. Otherwise, it displays the path cost to the root bridge from the designated port for the LAN segament to which this port is connected,
Root Guard State (Standalone mode)	This field displays the state of the port on which root guard is enabled. • **Root-inconsistent** - the Switch receives superior BPDUs on the port and blocks the port. • **Forwarding** - the Switch unbolcks and allows the port to forward frames again.

11.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 11.1 on page 132 for more information on MRSTP.

Figure 97 Advanced Application > Spanning Tree Protocol > MRSTP (Standalone mode)

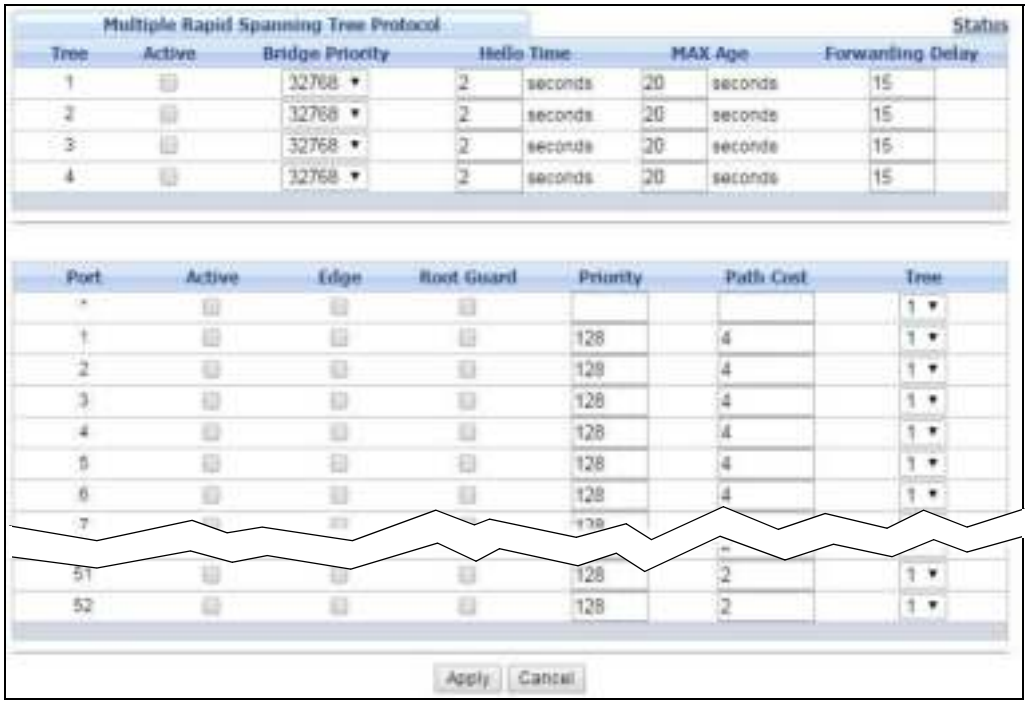
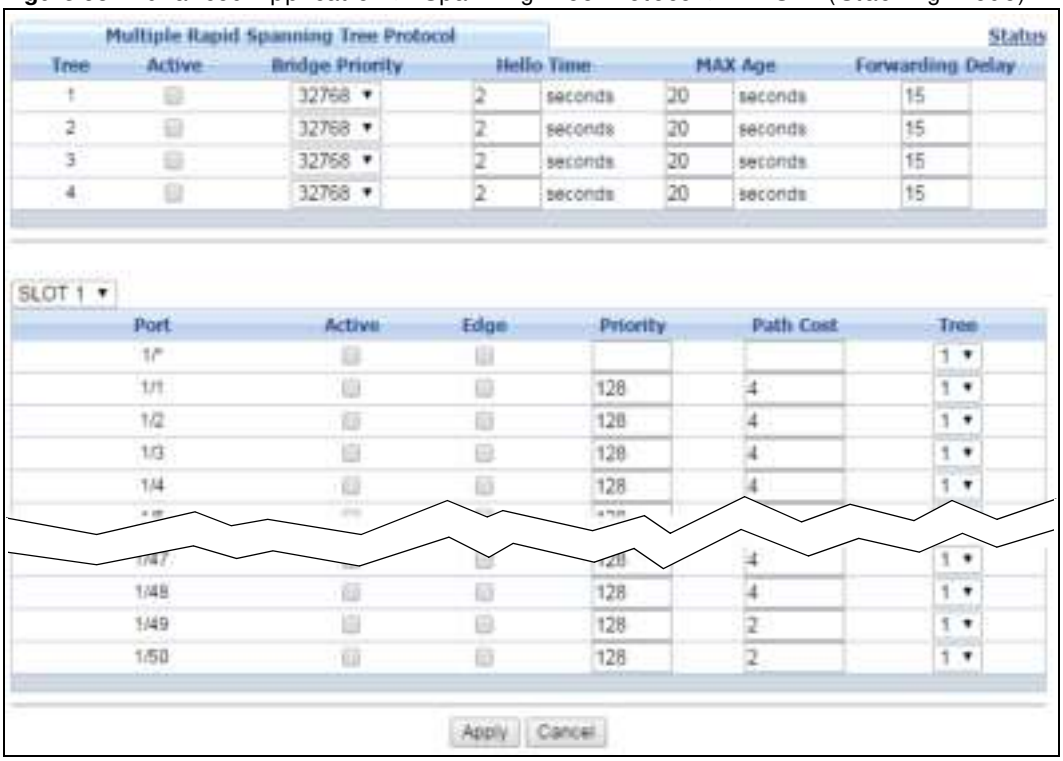


Figure 98 Advanced Application > Spanning Tree Protocol > MRSTP (Stacking mode)



The following table describes the labels in this screen.

Table 60 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MRSTP Status** screen (see Figure 99 on page 145).
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. Note: You must also activate **Multiple Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** 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) a 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) a 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 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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 STP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).

Table 60 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

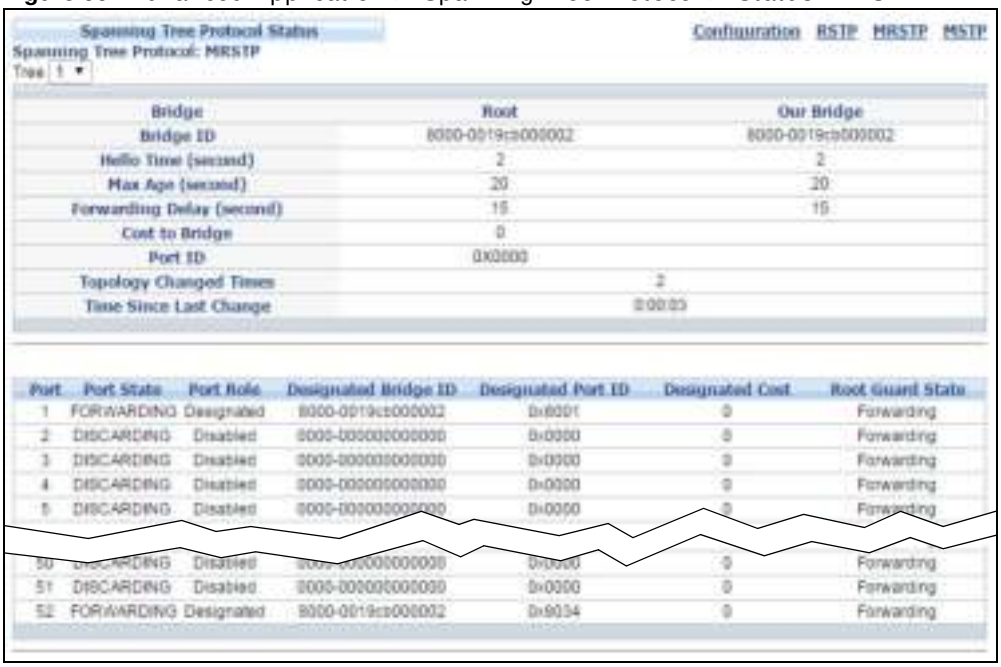
LABEL	DESCRIPTION
Root Guard (Standalone mode)	Select this check box to enable root guard on this port in order to prevent the switch(es) attached to the port from becoming the root bridge. With root guard enabled, a port is blocked when the Switch receives a superior BPDU on it. The Switch allows traffic to pass through this port again when the switch connected to the port stops to send superior BPDUs.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the 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 that you assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 55 on page 132 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.7 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 11.1 on page 132 for more information on MRSTP.

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

Figure 99 Advanced Application > Spanning Tree Protocol > Status: MRSTP



The following table describes the labels in this screen.

Table 61 Advanced Application > Spanning Tree Protocol > Status: MRSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MRSTP** to edit MRSTP settings on the Switch.
Tree	Select which STP tree configuration you want to view.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** 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 **Root** and **Our Bridge** 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) a 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). Note: 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.
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.
Port	This field displays the number of the port on the Switch.
Port State	This field displays the port state in STP. • **Discarding** - The port does not forward/process received frames or learn MAC addresses, but still listens for BPDUs. • **Learning** - The port learns MAC addresses and processes BPDUs, but does not forward frames yet. • **Forwarding** - The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.
Port Role	This field displays the role of the port in STP. • **Root** - A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does not have a root port. • **Designated** - A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • **Alternate** - A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • **Backup** - A blocked port, which has a backup/redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • **Disabled** - Not strictly part of STP. The port can be disabled manually.
Designated Bridge ID	This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected.
Designated Port ID	This field displays the priority and number of the bridge port (on the designated bridge), through which the designated bridge transmits the stored configuration messages.

Table 61 Advanced Application > Spanning Tree Protocol > Status: MRSTP (continued)

LABEL	DESCRIPTION
Designated Cost	This field displays the path cost to the LAN segment to which the port is connected when the port is a designated port. Otherwise, it displays the path cost to the root bridge from the designated port for the LAN segament to which this port is connected.
Root Guard State (Standalone mode)	This field displays the state of the port on which root guard is enabled. • **Root** - inconsistent - the Switch receives superior BPDUs on the port and blocks the port. • **Forwarding** - the Switch unbolcks and allows the port to forward frames again.

11.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 11.1.5 on page 134 for more information on MSTP.

Figure 100 Advanced Application > Spanning Tree Protocol > MSTP (Standalone mode)

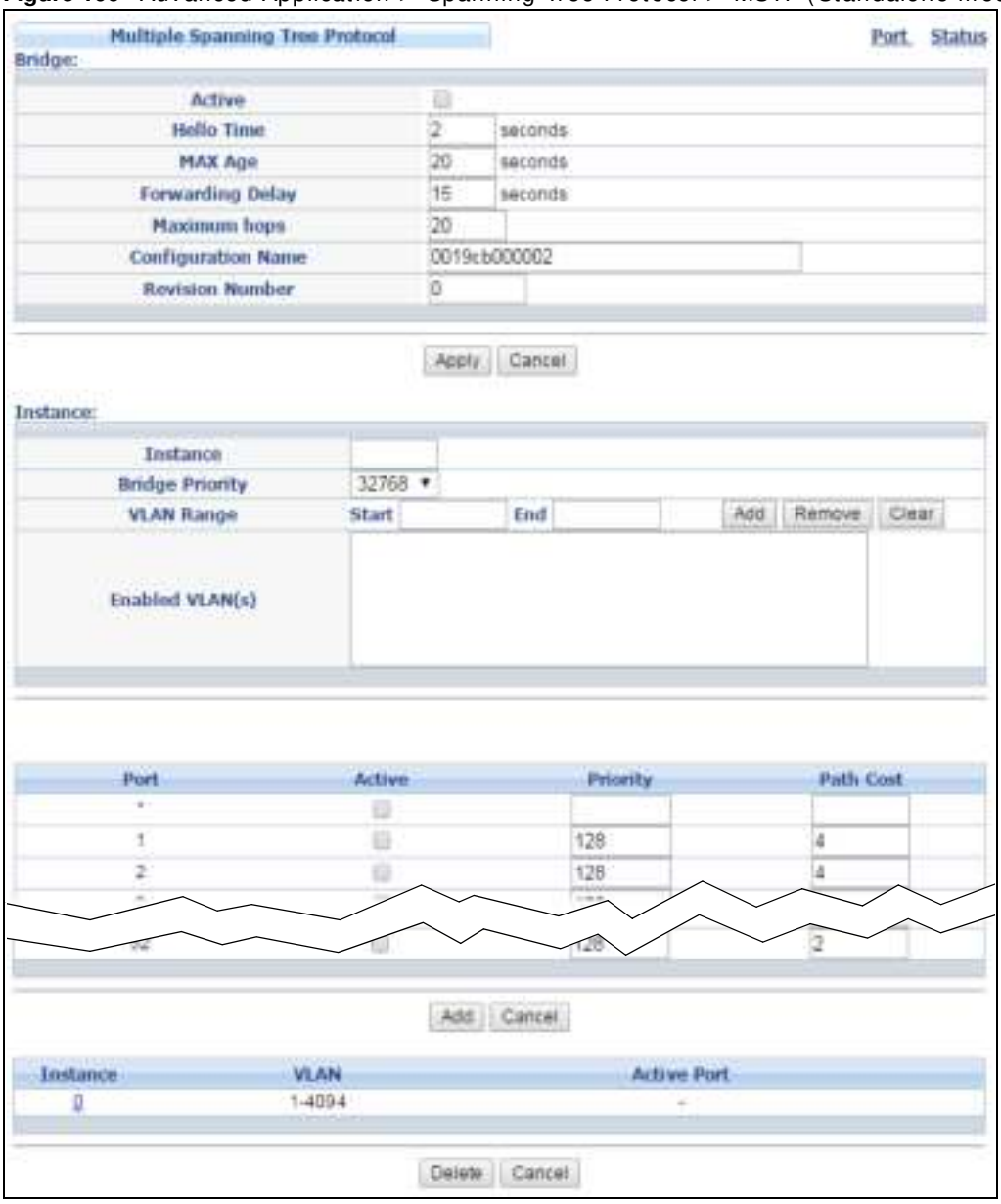
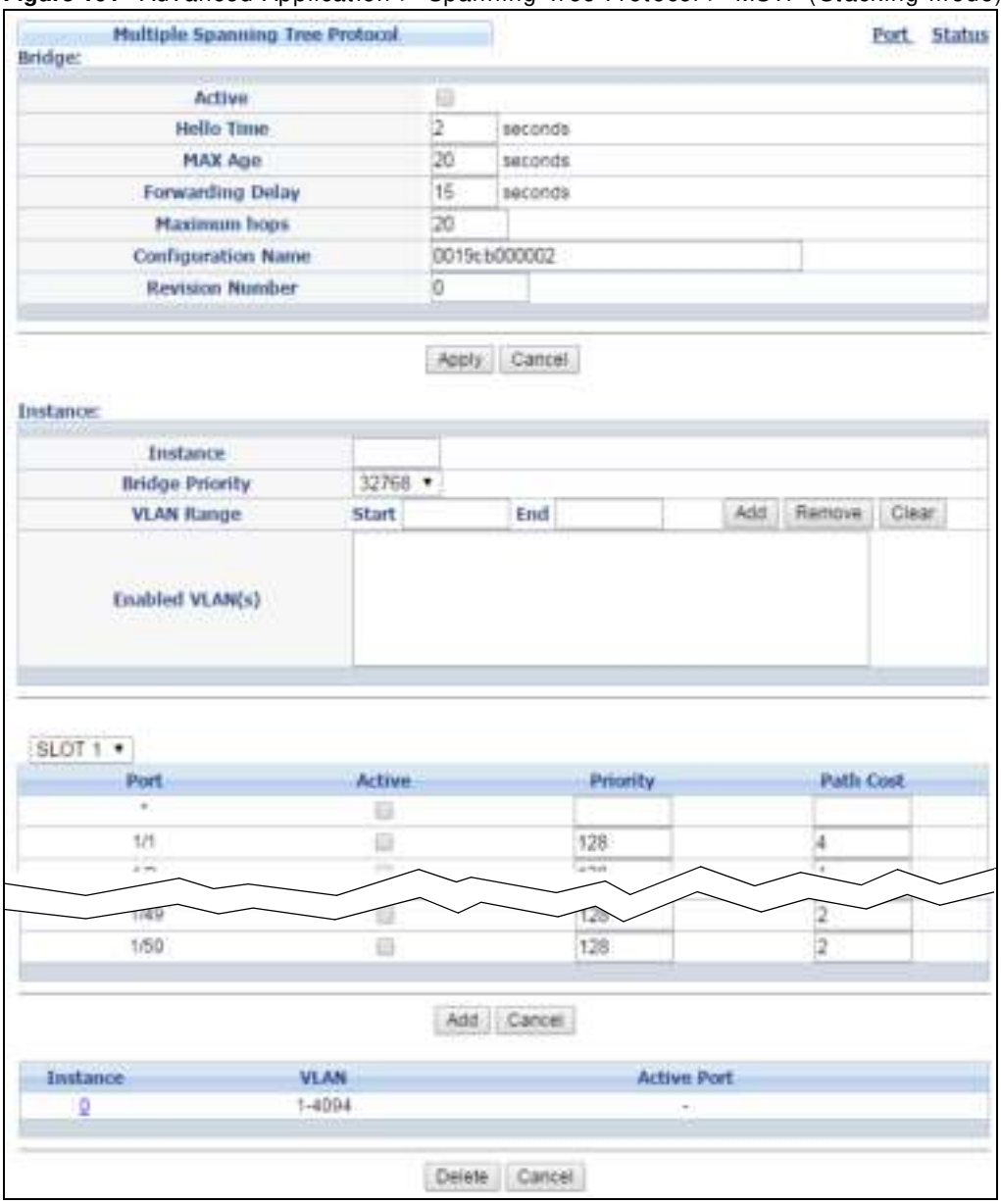


Figure 101 Advanced Application > Spanning Tree Protocol > MSTP (Stacking mode)



The following table describes the labels in this screen.

Table 62 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MSTP Status** screen (see Figure 104 on page 154).
Active	Select this check box to activate MSTP on the Switch. Clear this checkbox to disable MSTP on the Switch. Note: You must also activate **Multiple Spanning Tree** in the **Advanced Application > Spanning Tree Protocol > Configuration** 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.

Table 62 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
MaxAge	This is the maximum time (in seconds) a 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) a 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 * (Forward Delay - 1) >= Max Age >= 2 * (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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** 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 **Start** field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **End** field. Next click: • **Add** - to add this range of VLAN(s) to be mapped to the MST instance. • **Remove** - to remove this range of VLAN(s) from being mapped to the MST instance. • **Clear** - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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 62 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
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 the 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 Table 55 on page 132 for more information.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** 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.
	Select an entry's check box to select a specific entry.
Delete	Check the rule(s) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

11.8.1 Multiple Spanning Tree Protocol Port Configuration

To configure MSTP ports, click **Port** in the **Advanced Application** > **Spanning Tree Protocol** > **MSTP** screen.

Figure 102 Advanced Application > Spanning Tree Protocol > MSTP > Port (Standalone mode)

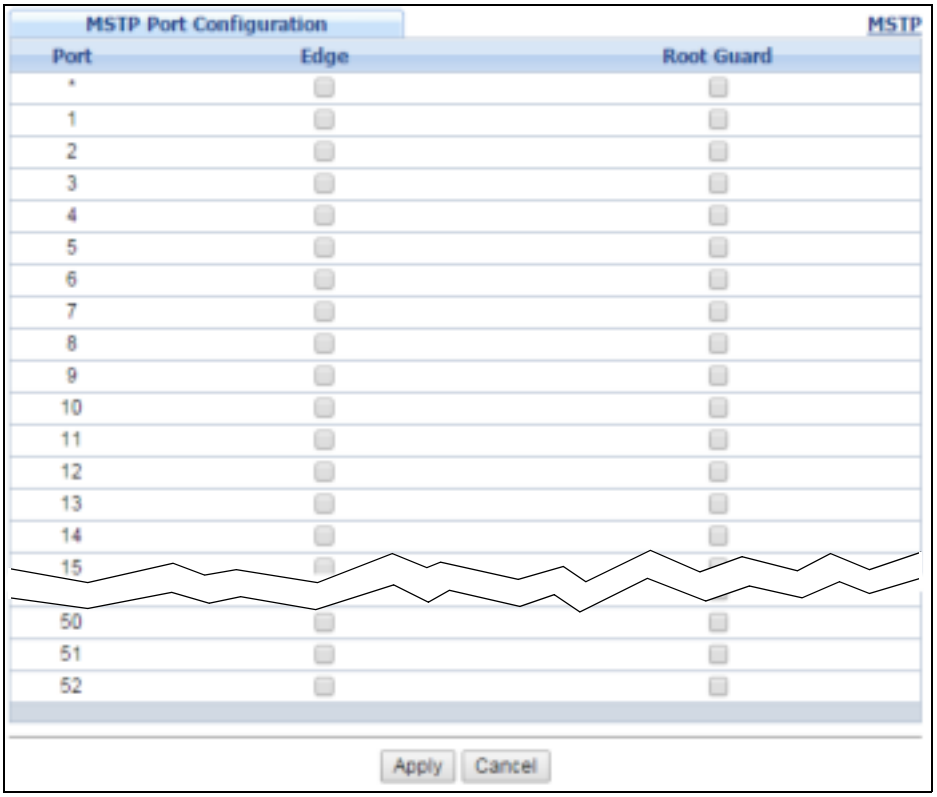
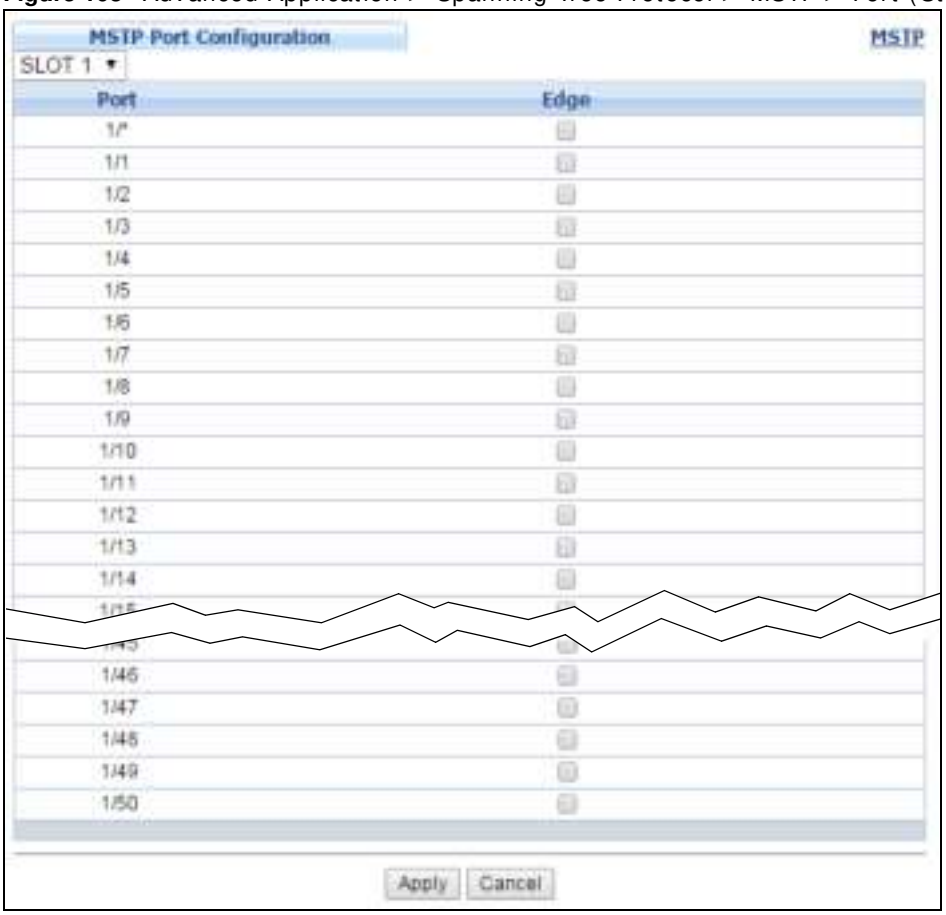


Figure 103 Advanced Application > Spanning Tree Protocol > MSTP > Port (Stacking mode)



The following table describes the labels in this screen.

Table 63 Advanced Application > Spanning Tree Protocol > MSTP > Port

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).

Table 63 Advanced Application > Spanning Tree Protocol > MSTP > Port (continued)

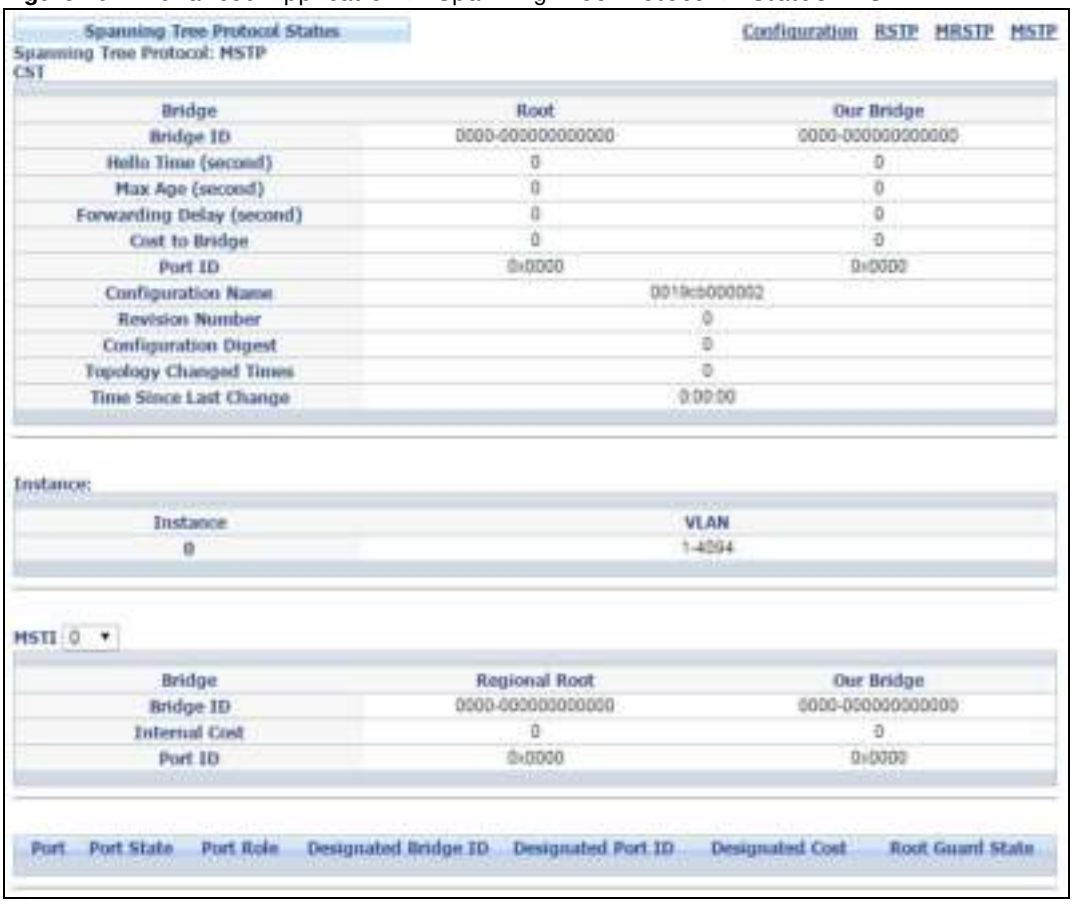
LABEL	DESCRIPTION
Root Guard (Standalone mode)	Select this check box to enable root guard on this port in order to prevent the switch(es) attached to the port from becoming the root bridge. With root guard enabled, a port is blocked when the Switch receives a superior BPDU on it. The Switch allows traffic to pass through this port again when the switch connected to the port stops to send superior BPDUs.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.9 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 11.1.5 on page 134 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



The following table describes the labels in this screen.

Table 64 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MSTP** to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** 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 **Root** and **Our Bridge** 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) a 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.
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	**Root** refers to the base of the MST instance. **Our Bridge** 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 **Root** and **Our Bridge** 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.
Port	This field displays the number of the port on the Switch.

Table 64 Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Port State	This field displays the port state in STP. • **Discarding** - The port does not forward/process received frames or learn MAC addresses, but still listens for BPDUs. • **Learning** - The port learns MAC addresses and processes BPDUs, but does not forward frames yet. • **Forwarding** - The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.
Port Role	This field displays the role of the port in STP. • **Root** - A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does not have a root port. • **Designated** - A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • **Alternate** - A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • **Backup** - A blocked port, which has a backup/redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • **Disabled** - Not strictly part of STP. The port can be disabled manually.
Designated Bridge ID	This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected.
Designated Port ID	This field displays the priority and number of the bridge port (on the designated bridge), through which the designated bridge transmits the stored configuration messages.
Designated Cost	This field displays the path cost to the LAN segment to which the port is connected when the port is a designated port. Otherwise, it displays the path cost to the root bridge from the designated port for the LAN segament to which this port is connected.
Root Guard State (Standalone mode)	This field displays the state of the port on which root guard is enabled. • **Root** - inconsistent - the Switch receives superior BPDUs on the port and blocks the port. • **Forwarding** - the Switch unbolcks and allows the port to forward frames again.

12

Bandwidth Control

This chapter shows you how to cap the maximum bandwidth using the **Bandwidth Control** screen.

12.1 Bandwidth Control Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

12.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.

Note: The CIR should be less than the PIR.

Note: The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

12.2 Bandwidth Control Setup

Click **Advanced Application** > **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 105 Advanced Application > Bandwidth Control (Standalone mode)

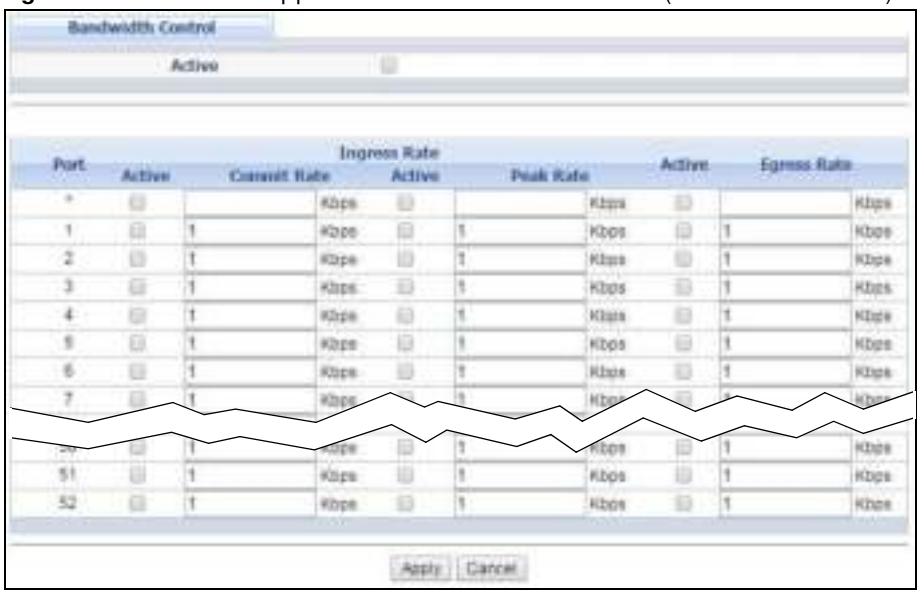
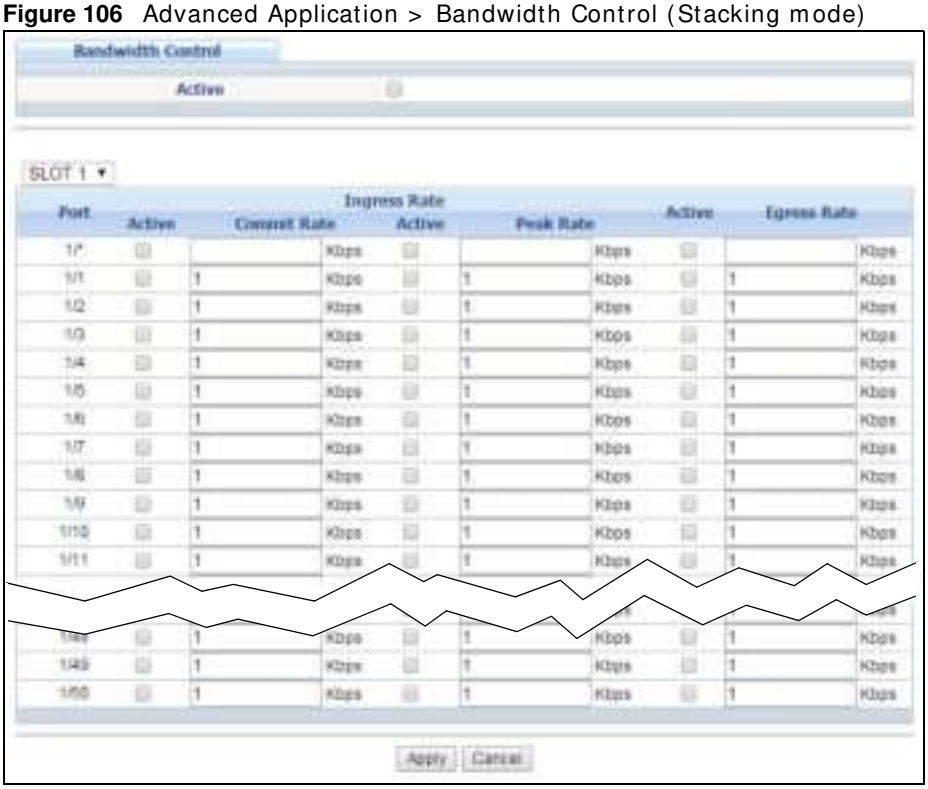


Figure 106 Advanced Application > Bandwidth Control (Stacking mode)



The following table describes the related labels in this screen.

Table 65 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.

Table 65 Advanced Application > Bandwidth Control (continued)

LABEL	DESCRIPTION
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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 Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13

Broadcast Storm Control

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

13.1 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 107 Advanced Application > Broadcast Storm Control (Standalone mode)

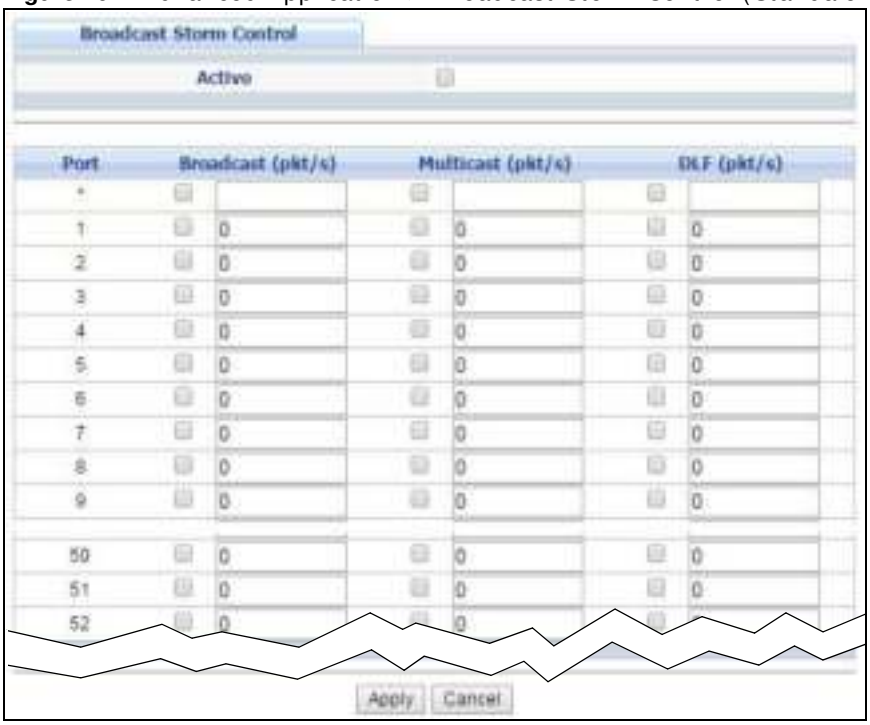
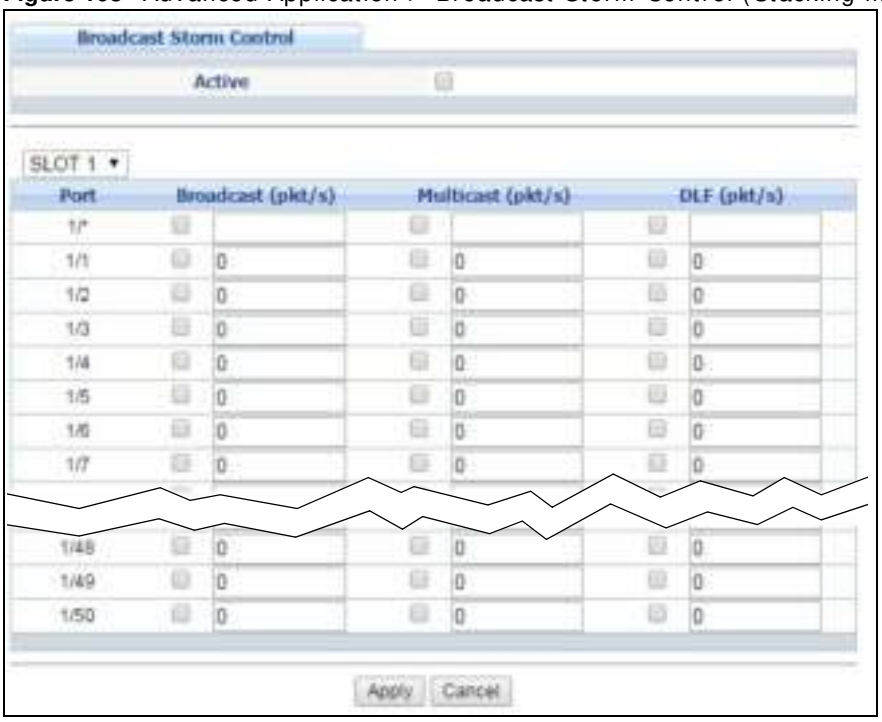


Figure 108 Advanced Application > Broadcast Storm Control (Stacking mode)



The following table describes the labels in this screen.

Table 66 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.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14 Mirroring

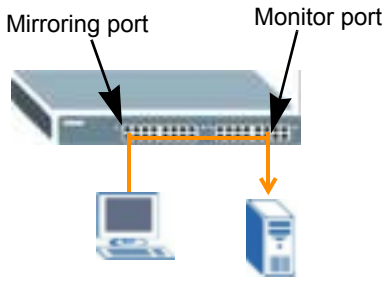
This chapter discusses port mirroring setup screens.

14.1 Port Mirroring

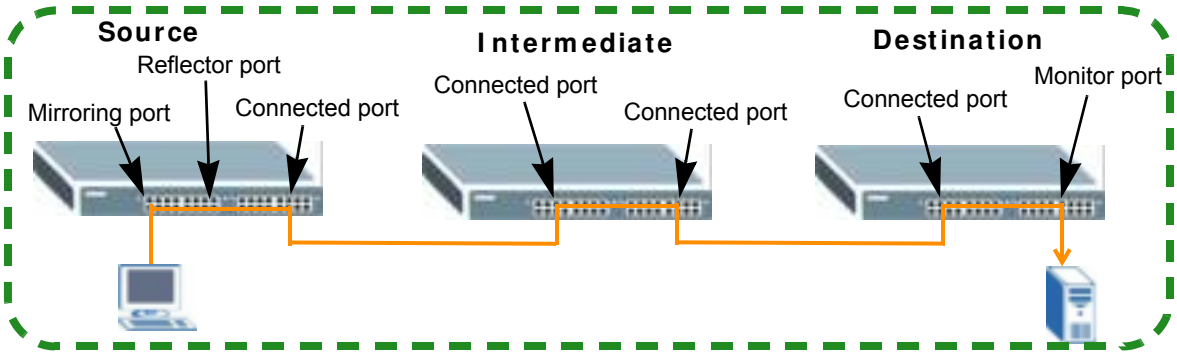
Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

The Switch supports both local port mirroring and remote port mirroring.

In local port mirroring, the mirroring ports (through which traffic you copy passes) and the monitor port are on the same device.



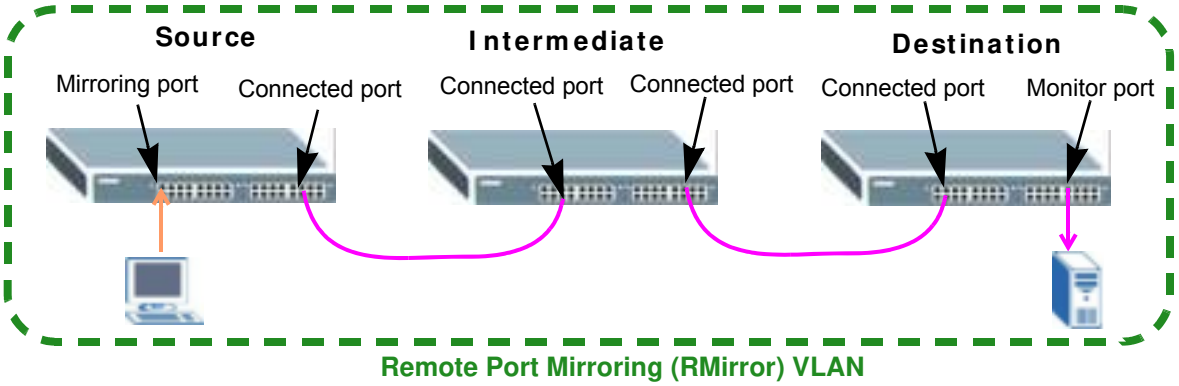
In remote port mirroring (RMirror), the mirroring ports and monitor port can be on different devices in a network. You can use it to monitor multiple switches across your network. The traffic from the source device's mirroring port(s) is sent to a reflector port for VLAN tagging and copied to the connected port(s). Traffic are then carried over the specified remote port mirroring (RMirror) VLAN and sent to the destination device's monitor port through the connected ports that connect to other switches.



Remote Port Mirroring (RMirror) VLAN

Single-Destination RMirror

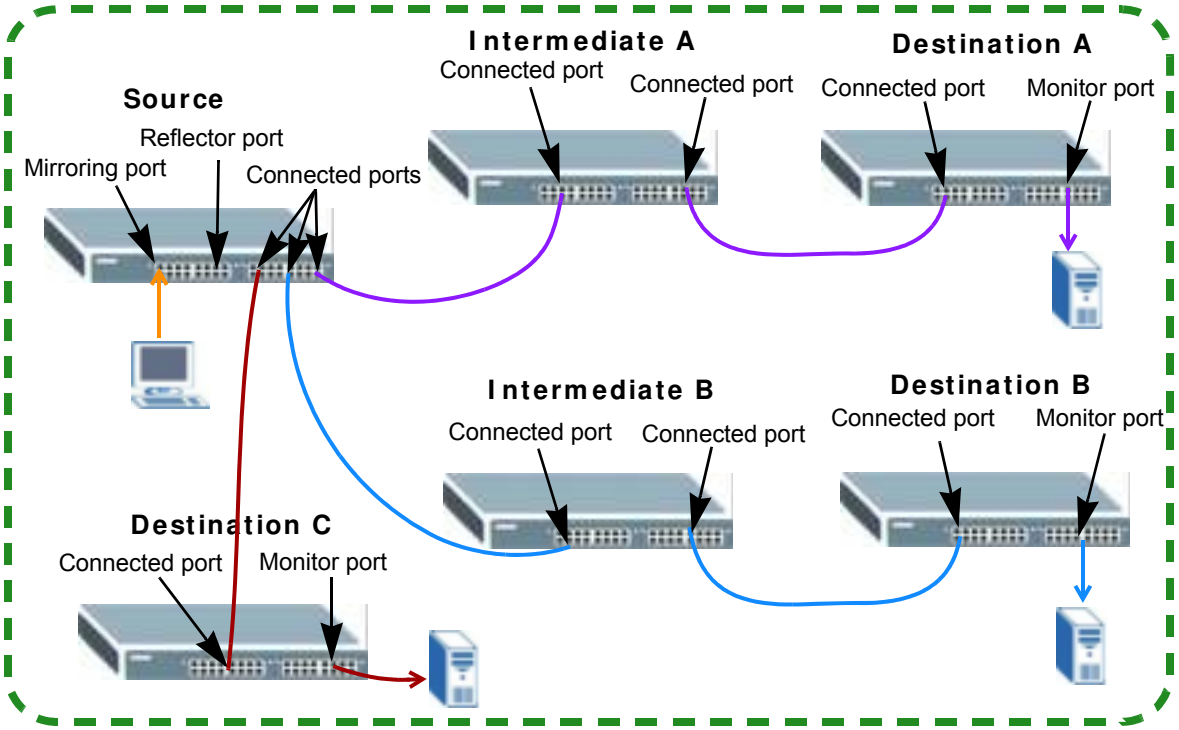
If the mirrored traffic is forwarded to one single destination switch, you can disable the reflector port. The Switch adds RMirror VLAN tag and forwards mirrored traffic from the mirroring port to the connected port directly.



Remote Port Mirroring (RMirror) VLAN

Multi-Destination RMirror

If you configure more than one connected port on the source switch to forward the mirrored traffic to multiple destination switches, you must enable a reflector port on the source switch.



Remote Port Mirroring (RMirror) VLAN

Port Rules in Port Mirroring

The following table shows the rule for a port in remote port mirroring. For example, a port on the source device can be a mirroring port in both RMirror VLAN 1 and RMirror VLAN 2. But when the port is the source device's mirroring port in RMirror VLAN 1, it cannot be the reflector port or monitor port in another RMirror VLAN.

Table 67 Port Rules between Different Remote Port Mirroring VLANs

		RMirror VLAN 1				
		Source Mirroring Port	**Source Reflector Port**	**Connected Port**	**Source Connected Port in Single-Destination RMirror**	**Destination Monitor Port**
RMirror VLAN 2	**Source Mirroring Port**	Y	N	Y	N	N
	Source Reflector Port	N	N	N	N	N
	Connected Port	Y	N	Y	Y	N
	Source Connected Port in Single-Destination RMirror	N	N	Y	N	N
	Destination Monitor Port	N	N	N	N	N

The following table shows the rule for a port used in both local port mirroring and remote port mirroring. For example, the RMirror mirroring port on the source device can also be used as the mirroring port in local port mirroring. But it cannot be the monitor port in local port mirroring.

Table 68 Port Rules between Remote and Local Port Mirroring

		RMirror				
		Source Mirroring Port	**Source Reflector Port**	**Connected Port**	**Source Connected Port in Single-Destination RMirror**	**Destination Monitor Port**
Local Port Mirroring	**Mirroring Port**	Y	N	Y	N	N
	Monitor Port	N	N	N	N	N

14.1.1 Local Port Mirroring

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 109 Advanced Application > Mirroring (Standalone mode)

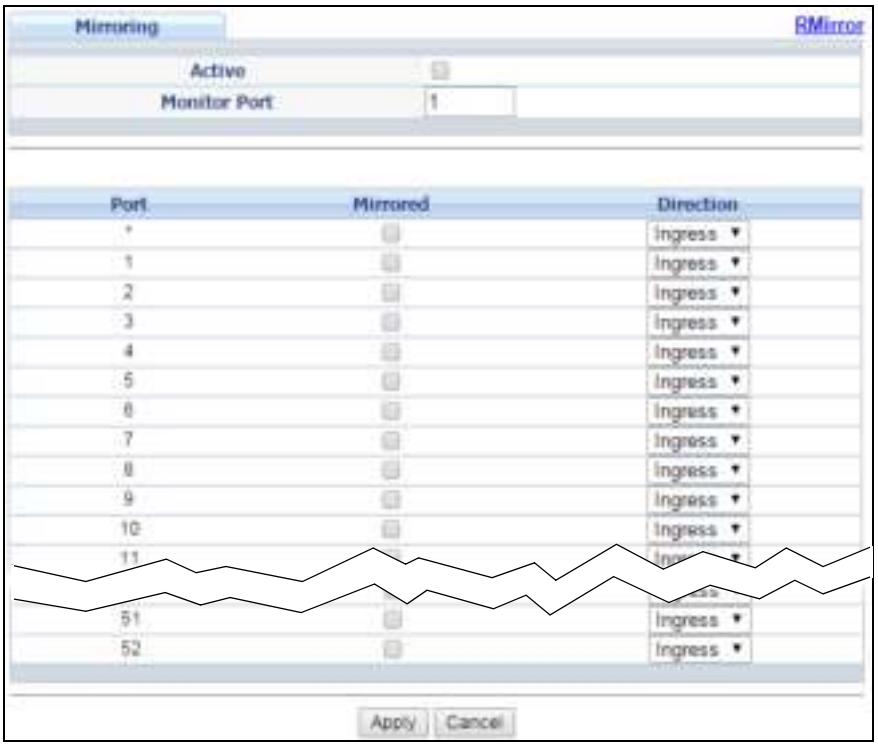
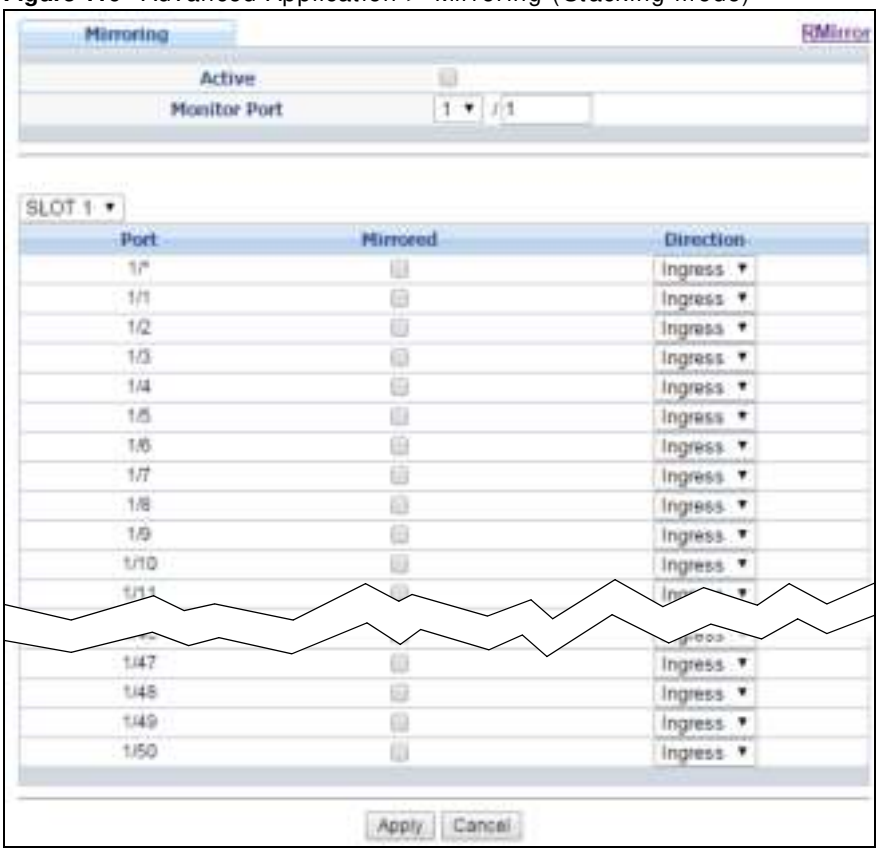


Figure 110 Advanced Application > Mirroring (Stacking mode)



The following table describes the labels in this screen.

Table 69 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). Type the port number of the monitor port. In stacking mode, the first number represents the slot and the second the port number.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
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 **Egress** (outgoing), **Ingress** (incoming) and **Both**.

Table 69 Advanced Application > Mirroring (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.1.2 Remote Port Mirroring

Use this screen to create a remote port mirroring (RMirror) VLAN through which the mirrored traffic is forwarded.

Click the **RMirror** link in the **Advanced Application** > **Mirroring** screen. The following screen opens.

Figure 111 Advanced Application > Mirroring > RMirror

The following table describes the labels in this screen.

Table 70 Advanced Application > Mirroring > RMirror

LABEL	DESCRIPTION
Active	Select the option to enable the VLAN.
RMirror VLAN ID	Specify the ID number of remote port mirroring (RMirror) VLAN.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the ID number of the RMirror VLAN. Click on the VLAN ID number to change the settings.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Active	This field displays whether the VLAN is enabled or not.
Delete	Check the rule(s) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

14.1.3 Source

Use this screen to configure the reflector port and specify the traffic flow to be copied to the monitor port when the Switch is the source device in remote port mirroring.

Click the **Source** link in the **RMirror** screen. The following screen opens.

Figure 112 Advanced Application > Mirroring > RMirror > Source (Standalone mode)

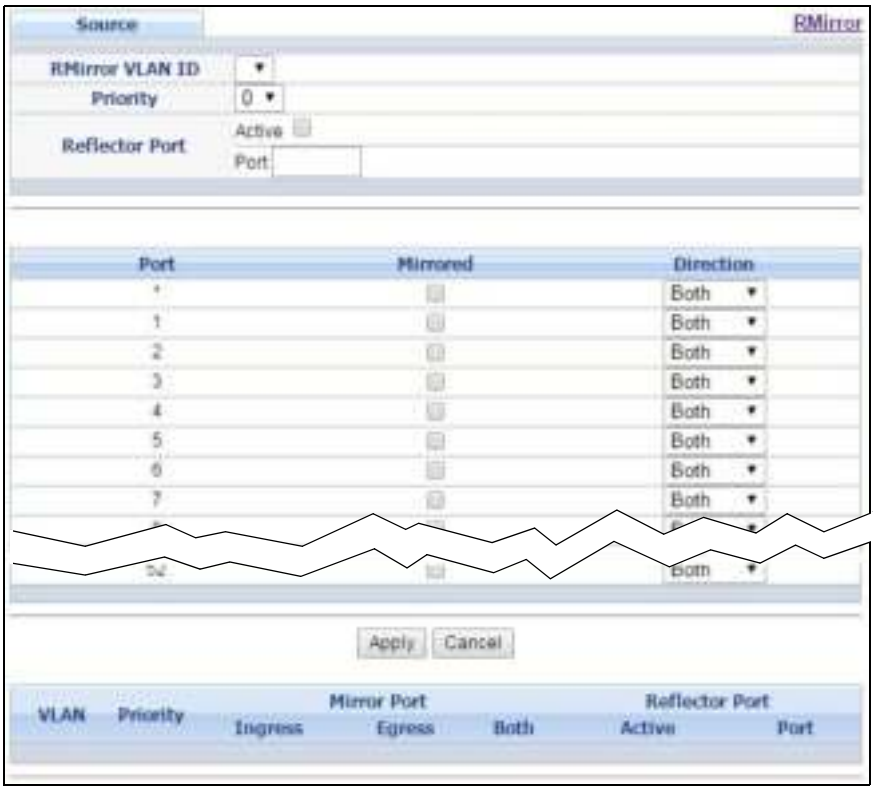
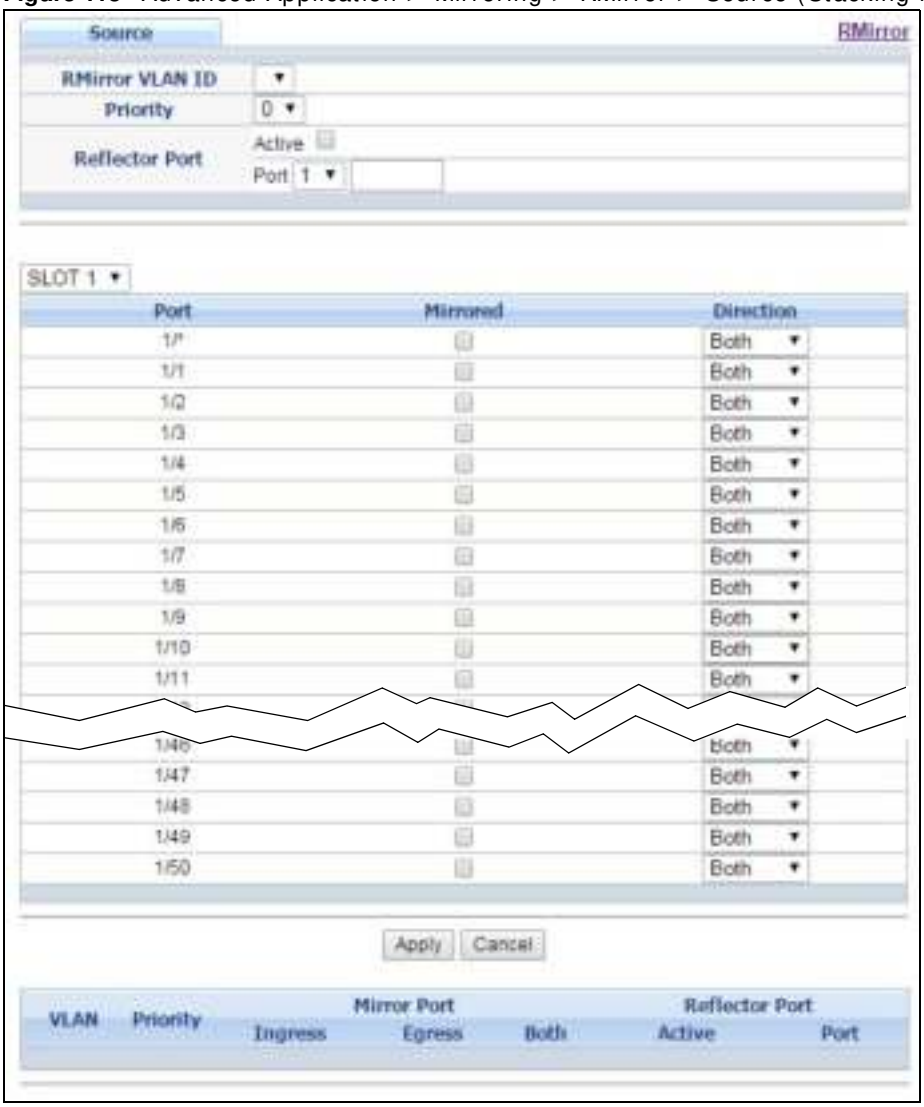


Figure 113 Advanced Application > Mirroring > RMirror > Source (Stacking mode)



The following table describes the labels in this screen.

Table 71 Advanced Application > Mirroring > RMirror > Source

LABEL	DESCRIPTION
RMirror VLAN ID	Select the RMirror VLAN over which the mirrored traffic is forwarded.
Priority	Enter the priority of the mirrored traffic.
Reflector Port	Select the check box to enable the specified reflector port. Enter the number of reflector port that adds the RMirror VLAN tag to all mirrored traffic and forwards traffic to the connected port(s) in the same RMirror VLAN.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 71 Advanced Application > Mirroring > RMirror > Source (continued)

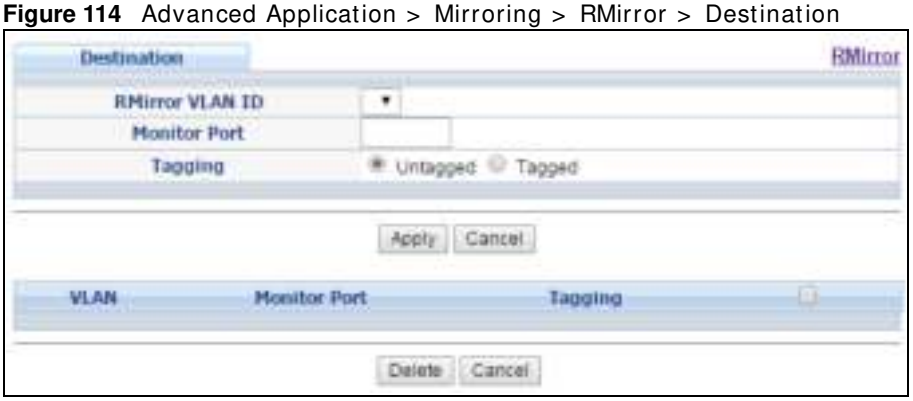
LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you 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 **Egress** (outgoing), **Ingress** (incoming) and **Both**.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the ID number of RMirror VLAN over which the mirrored traffic is forwarded.
Priority	This field displays the priority of the mirrored traffic.
Mirror Port	
Ingress	This field displays the number of port(s) on which the incoming traffic is mirrored.
Egress	This field displays the number of port(s) on which the outgoing traffic is mirrored.
Both	This field displays the number of port(s) on which the incoming and outgoing traffic is mirrored.
Reflector Port	This field displays whether the reflector port is enabled and the number of reflector port in this RMirror VLAN.

14.1.4 Destination

Use this screen to specify the RMirror VLAN and configure the monitor port when the Switch is the destination device in remote port mirroring.

Click the **Destination** link in the **RMirror** screen. The following screen opens.

Figure 114 Advanced Application > Mirroring > RMirror > Destination



The following table describes the labels in this screen.

Table 72 Advanced Application > Mirroring > RMirror > Destination

LABEL	DESCRIPTION
RMirror VLAN ID	Select the RMirror VLAN over which the mirrored traffic is forwarded.
Monitor Port	Specify the port to which you copy the traffic in order to examine it in more detail without interfering with the traffic flow on the original port(s).
Tagging	Select whether to add the RMirror VLAN tag to mirrored traffic on the monitor port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the ID number of RMirror VLAN over which the mirrored traffic is forwarded.
Monitor Port	This field displays the number of port that receives the mirrored traffic from the source device for analysis.
Tagging	This field displays whether the mirrored traffic is tagged with the RMirror VLAN ID.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.1.5 Connected Port

Use this screen to select the RMirror VLAN and specify the port(s) that helps forward mirrored traffic to other connected switches and/or receive mirrored traffic from other connected port in the same RMirror VLAN.

Click the **Connected Port** link in the **RMirror** screen. The following screen opens.

Figure 115 Advanced Application > Mirroring > RMirror > Connected Port (Standalone mode)

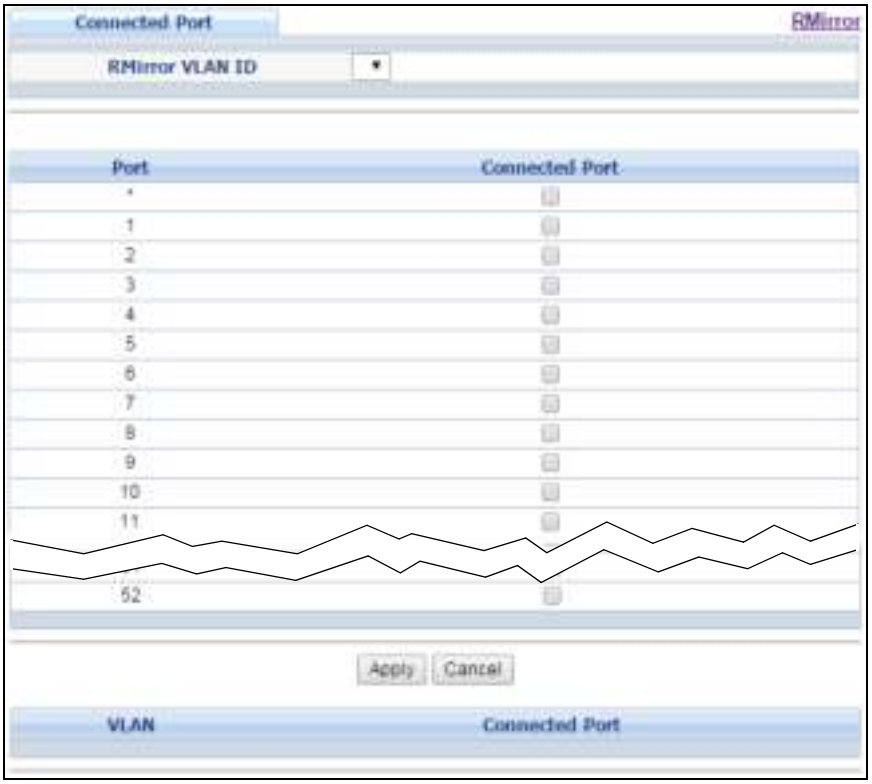
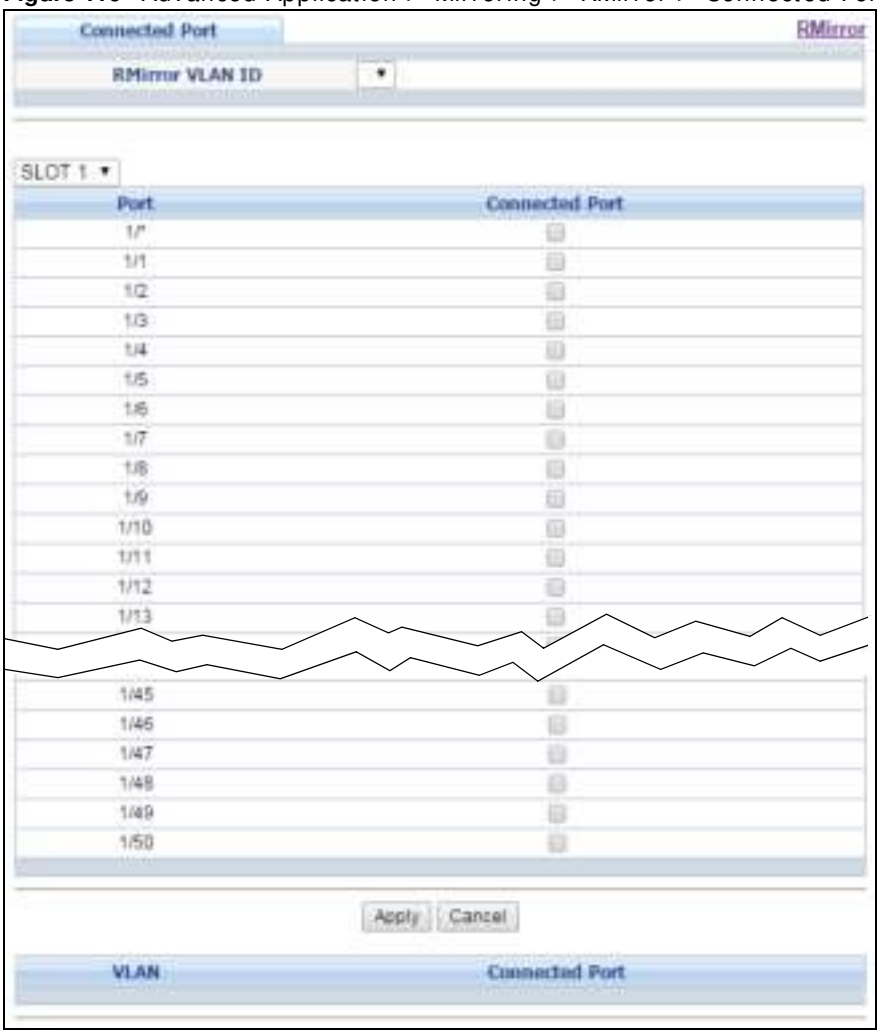


Figure 116 Advanced Application > Mirroring > RMirror > Connected Port (Stacking mode)



The following table describes the labels in this screen.

Table 73 Advanced Application > Mirroring > RMirror > Connected Port

LABEL	DESCRIPTION
RMirror VLAN ID	Select the RMirror VLAN over which the mirrored traffic is forwarded.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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 73 Advanced Application > Mirroring > RMirror > Connected Port (continued)

LABEL	DESCRIPTION
Connected Port	When the Switch is a source device in remote port mirroring, select this option to have the port help forward mirrored traffic to the connected port of the intermediate or destination device in the same RMirror VLAN. When the Switch is an intermediate device in remote port mirroring, select this option to have the port receive mirrored traffic from the connected source or another intermediate device or forward mirrored traffic to the connected destination or another intermediate device in the same RMirror VLAN. When the Switch is a destination device in remote port mirroring, select this option to have the port receive mirrored traffic from the connected source or intermediate device in the same RMirror VLAN.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the ID number of port mirroring VLAN over which the mirrored traffic is forwarded.
Connected Port	This field displays the number of port(s) that helps forward mirrored traffic to other connected switches.

15

Link Aggregation

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

15.1 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 15.6 on page 183 for a static port trunking example.

15.2 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.

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

Table 74 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 75 Link Aggregation ID: Peer Switch

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

15.3 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See Section 15.1 on page 175 for more information.

Figure 117 Advanced Application > Link Aggregation Status

The following table describes the labels in this screen.

Table 76 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group 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 **Link Aggregation** screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this 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 Section 15.2.1 on page 176 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. **src-mac** means the Switch distributes traffic based on the packet's source MAC address. **dst-mac** means the Switch distributes traffic based on the packet's destination MAC address. **src-dst-mac** means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. **src-ip** means the Switch distributes traffic based on the packet's source IP address. **dst-ip** means the Switch distributes traffic based on the packet's destination IP address. **src-dst-ip** means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how these ports were added to the trunk group. It displays: • **Static** - if the ports are configured as static members of a trunk group. • **LACP** - if the ports are configured to join a trunk group via LACP.

15.4 Link Aggregation Setting

Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** to display the screen shown next. See Section 15.1 on page 175 for more information on link aggregation.

Figure 118 Advanced Application > Link Aggregation > Link Aggregation Setting (Standalone mode)

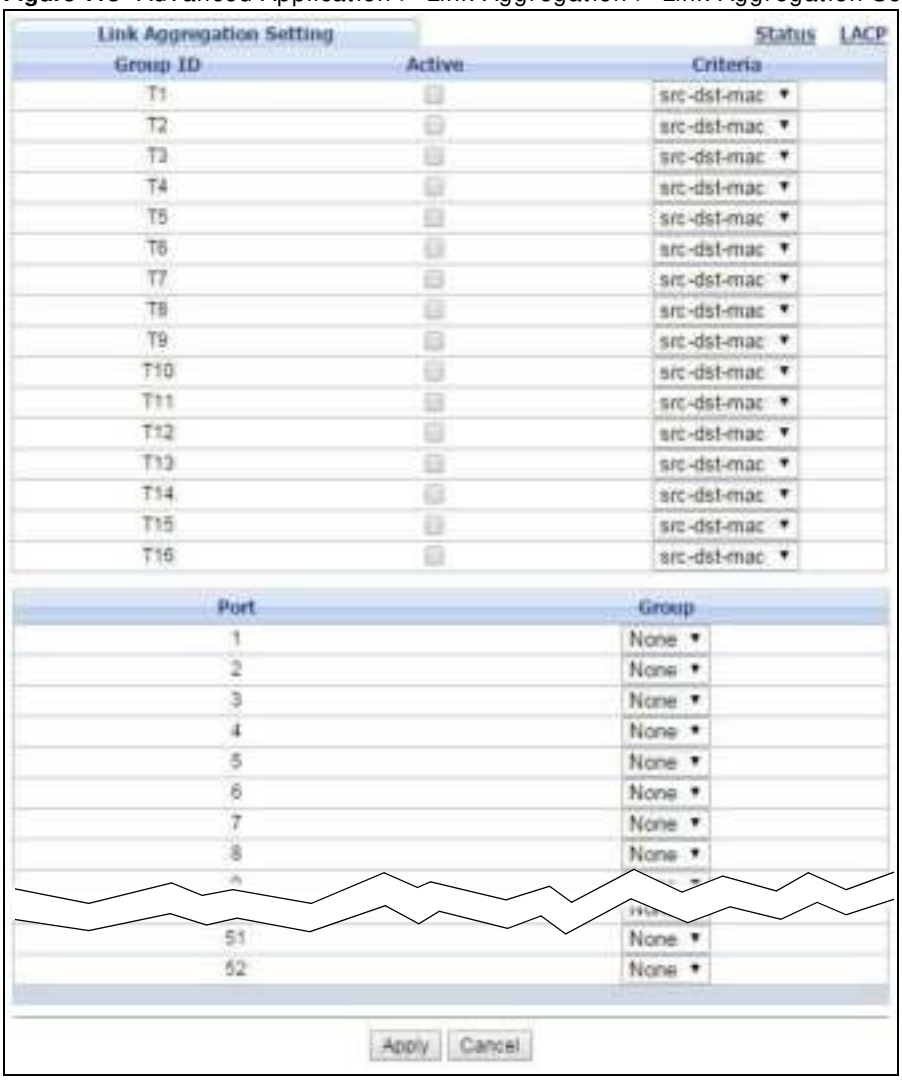
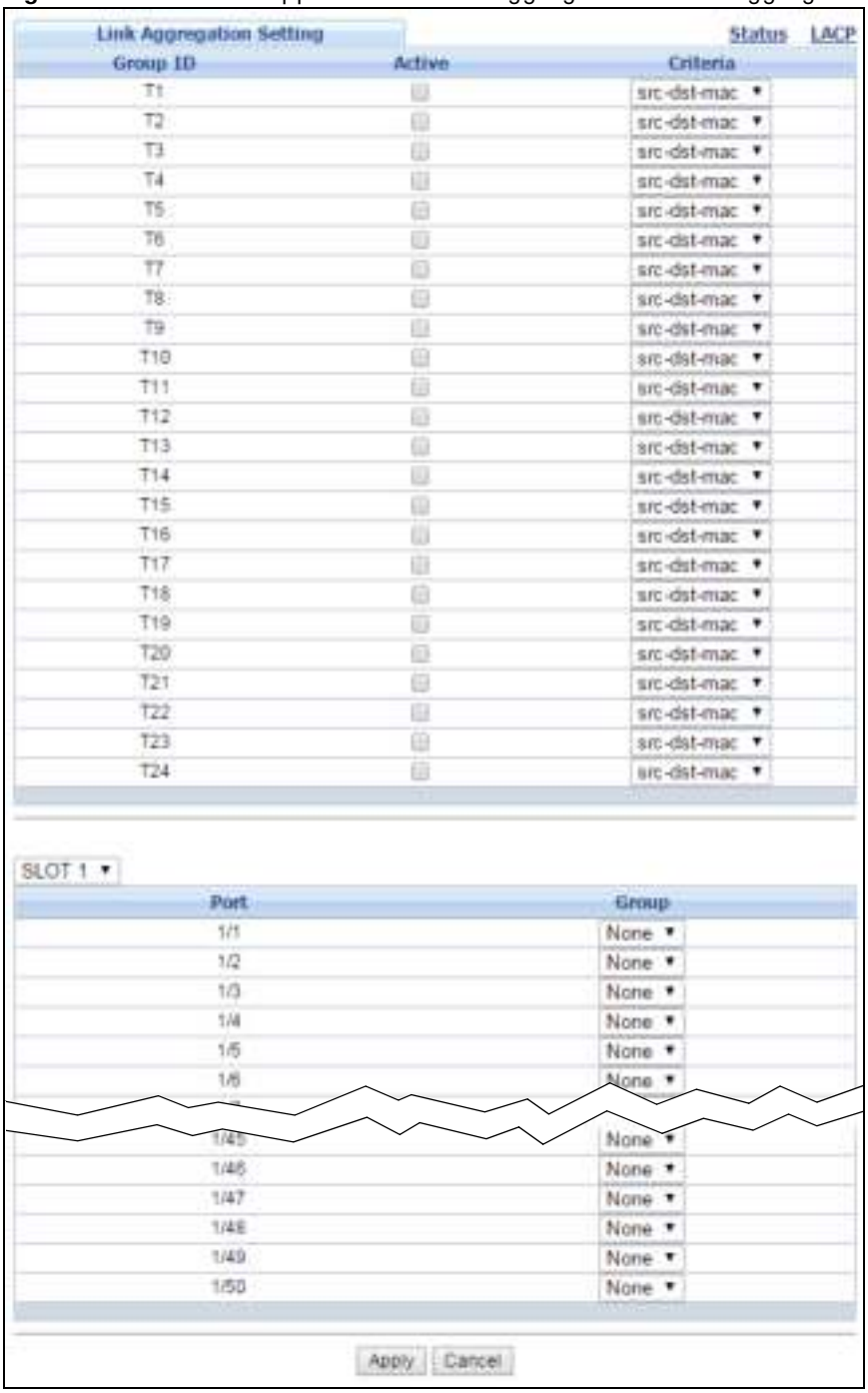


Figure 119 Advanced Application > Link Aggregation > Link Aggregation Setting (Stacking mode)



The following table describes the labels in this screen.

Table 77 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.

Table 77 Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

LABEL	DESCRIPTION
Active	Select this option to activate a trunk group.
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **src-dst-mac** distribution type. If the Switch is behind a router, the packet's destination or source MAC address will be changed. In this case, set the Switch to distribute traffic based on its IP address to make sure port trunking can work properly. Select **src-mac** to distribute traffic based on the packet's source MAC address. Select **dst-mac** to distribute traffic based on the packet's destination MAC address. Select **src-dst-mac** to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select **src-ip** to distribute traffic based on the packet's source IP address. Select **dst-ip** to distribute traffic based on the packet's destination IP address. Select **src-dst-ip** to distribute traffic based on a combination of the packet's source and destination IP addresses.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
Group	Select the trunk group to which a port belongs. Note: When you enable the port security feature on the Switch and configure port security settings for a port, you cannot include the port in an active trunk group.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.5 Link Aggregation Control Protocol

Click in the **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP** to display the screen shown next. See Section 15.2 on page 175 for more information on dynamic link aggregation.

Figure 120 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (Standalone mode)

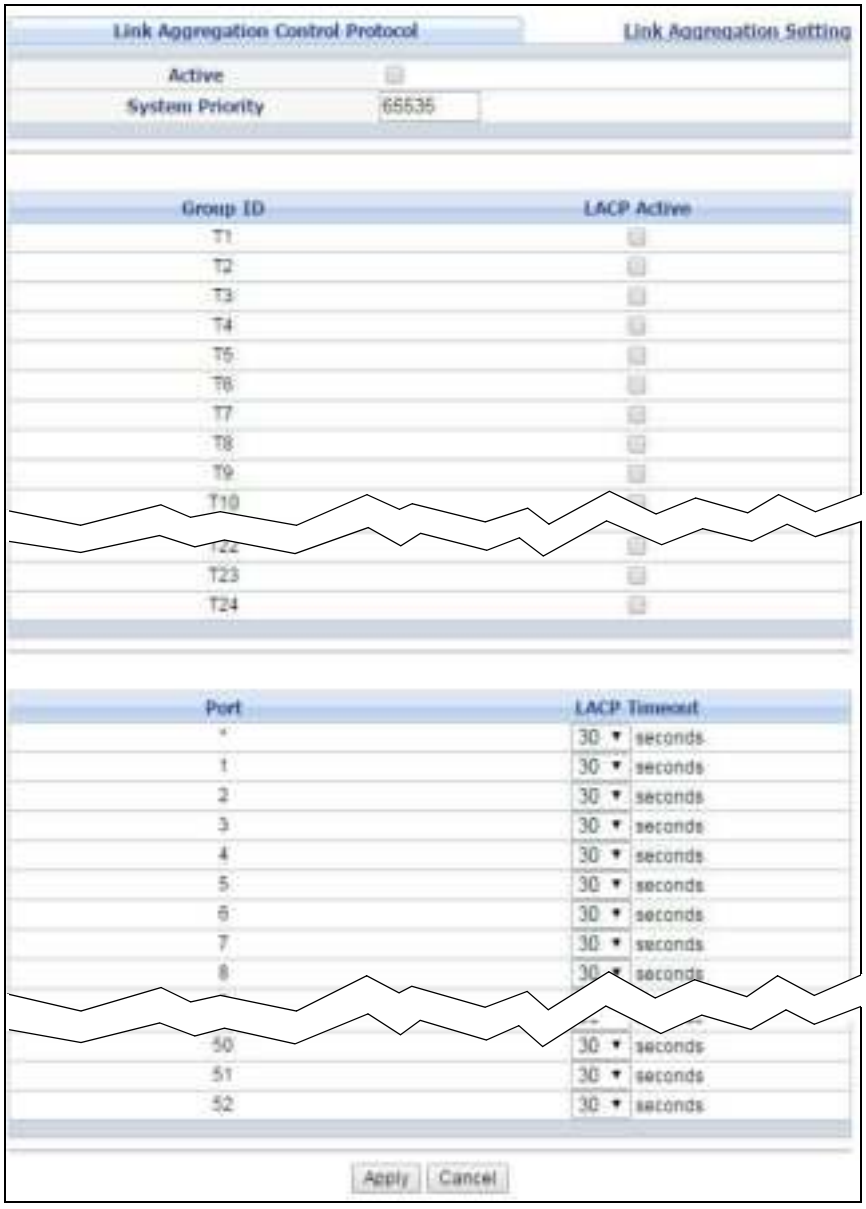


Figure 121 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (Stacking mode)

The following table describes the labels in this screen.

Table 78 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
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.

Table 78 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

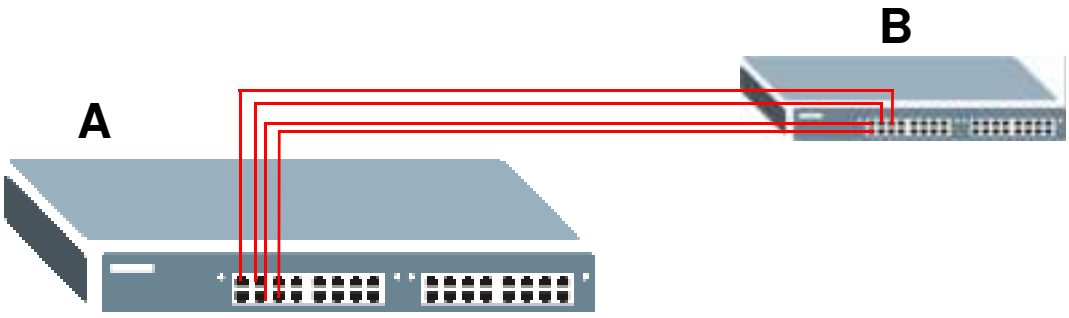
LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.6 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

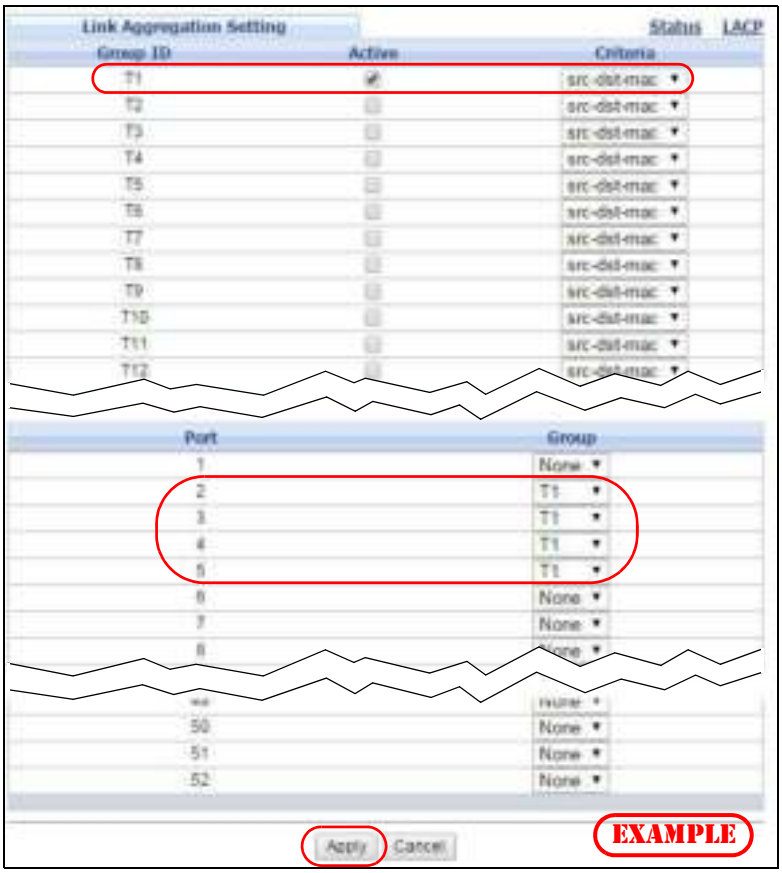
1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

Figure 122 Trunking Example - Physical Connections



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

Figure 123 Trunking Example - Configuration Screen



Your trunk group 1 (**T1**) configuration is now complete.

16

Port Authentication

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

16.1 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 - An authentication server validates access to a port based on a username and password provided by the user. 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.

- **MAC** - An authentication server validates access to a port based on the MAC address and password of the client.

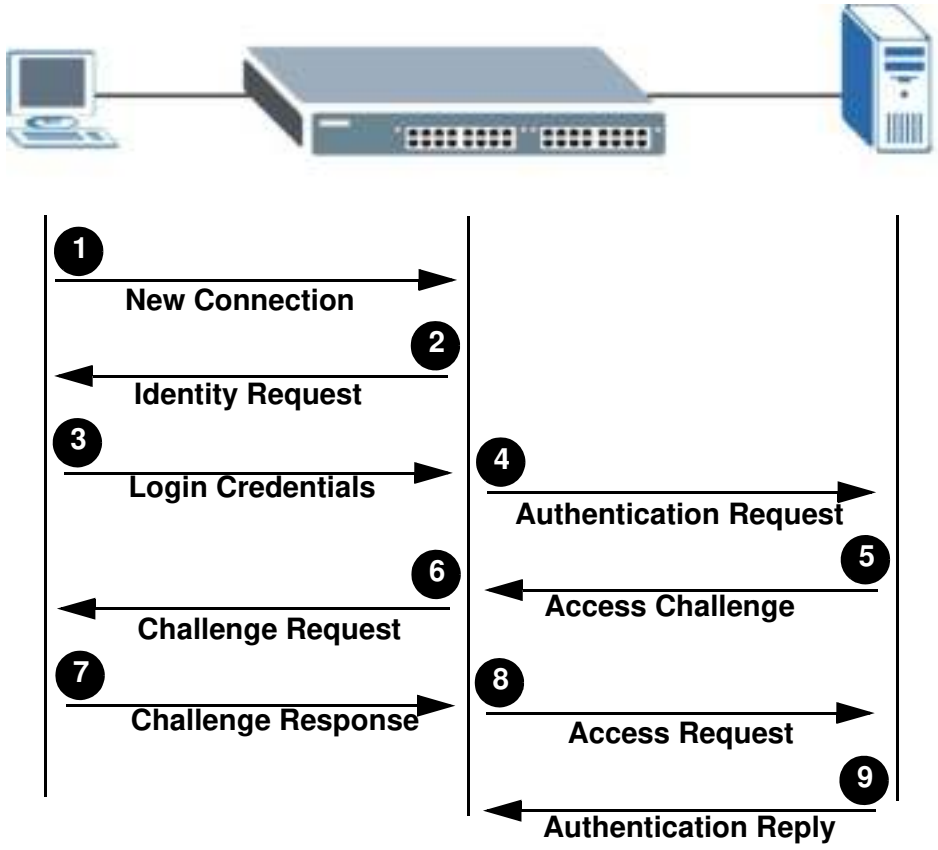
Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See Section 24.1.2 on page 254 for more information on configuring your RADIUS server settings.

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.

16.1.1 IEEE 802.1x Authentication

The following figure illustrates how a client connecting to an 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 after the client responds to its identity request. When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

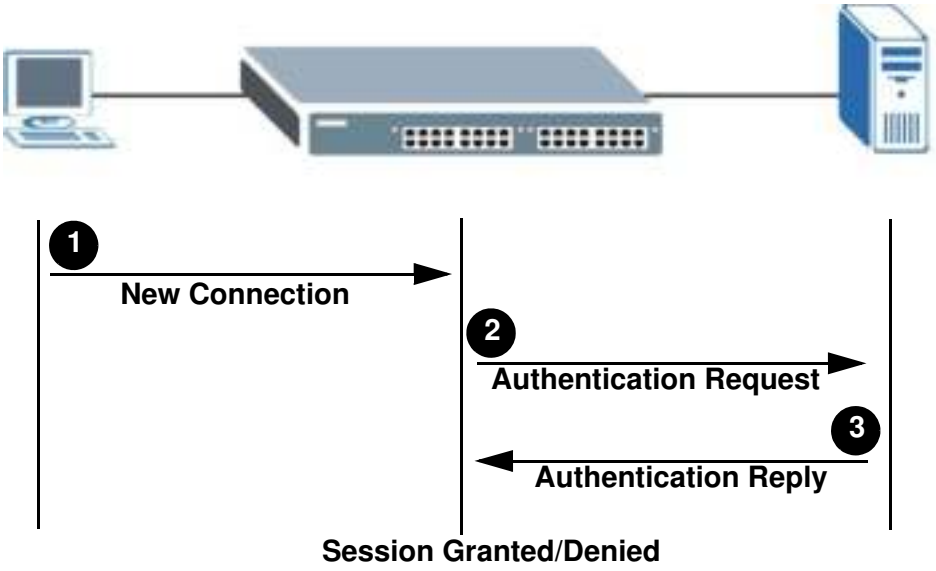
Figure 124 IEEE 802.1x Authentication Process



16.1.2 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 125 MAC Authentication Process



16.2 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 **AAA > Radius Server Setup** screen.

To activate a port authentication method, click **Advanced Application** > **Port Authentication** in the navigation panel. Select a port authentication method in the screen that appears.

Figure 126 Advanced Application > Port Authentication

16.2.1 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 127 Advanced Application > Port Authentication > 802.1x (Standalone mode)

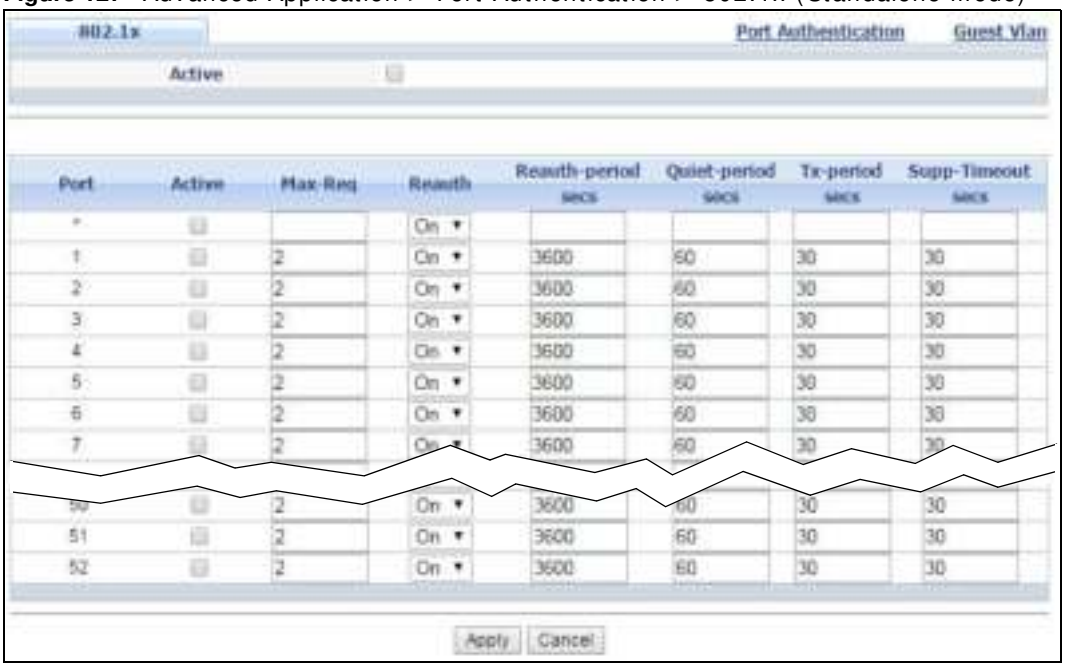
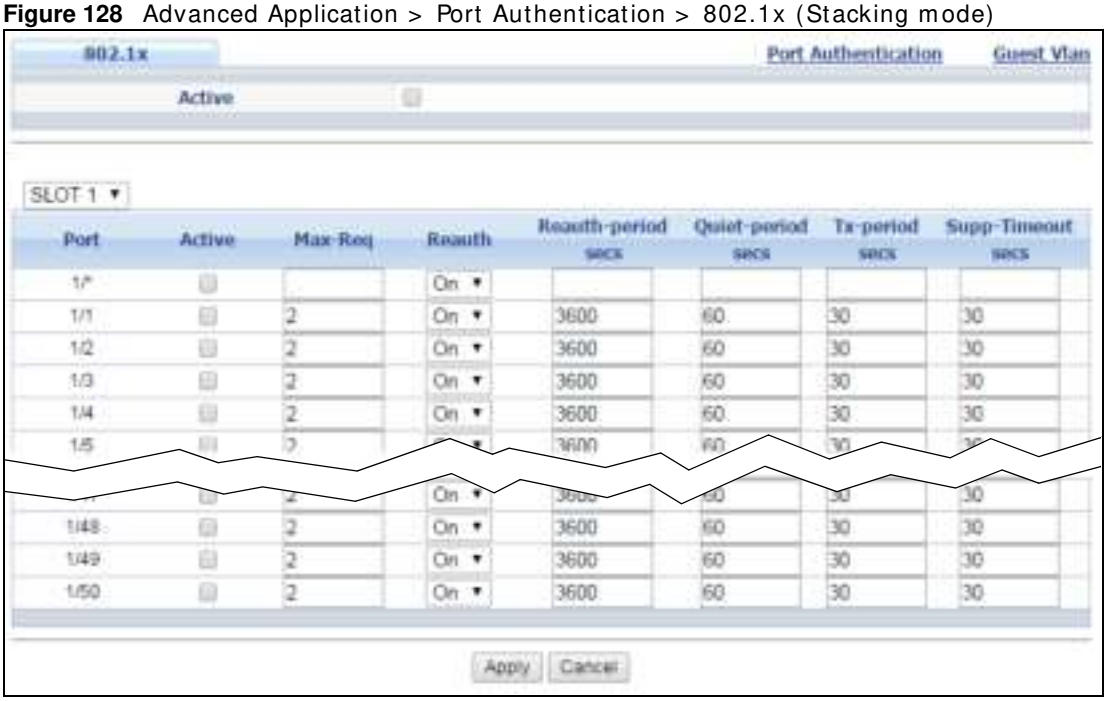


Figure 128 Advanced Application > Port Authentication > 802.1x (Stacking mode)



The following table describes the labels in this screen.

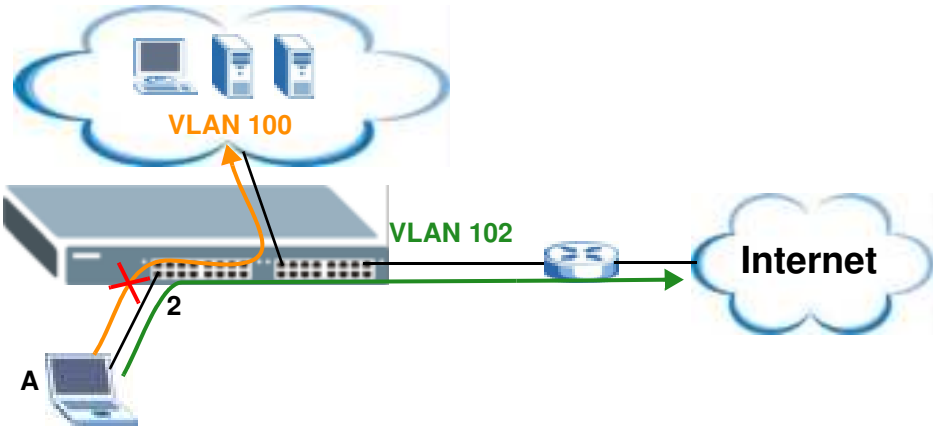
Table 79 Advanced Application > Port Authentication > 802.1x

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.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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 checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Max-Req	Specify the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.
Reauth	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-period	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Quiet-period	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.2.2 Guest VLAN

When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in the example), the user (**A** in the example) that is not IEEE 802.1x capable or fails to enter the correct username and password can still access the port, but traffic from the user is forwarded to the guest VLAN. That is, unauthenticated users can have access to limited network resources in the same guest VLAN, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 129 Guest VLAN Example



Use this screen to enable and assign a guest VLAN to a port. In the **Port Authentication > 802.1x** screen click **Guest Vlan** to display the configuration screen as shown.

Figure 130 Advanced Application > Port Authentication > 802.1x > Guest VLAN (Standalone mode)

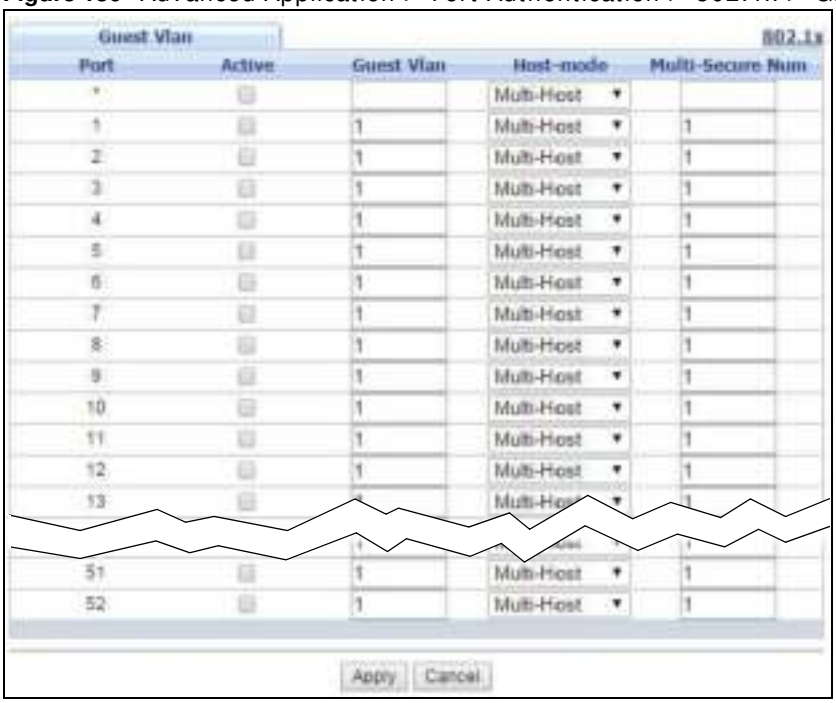
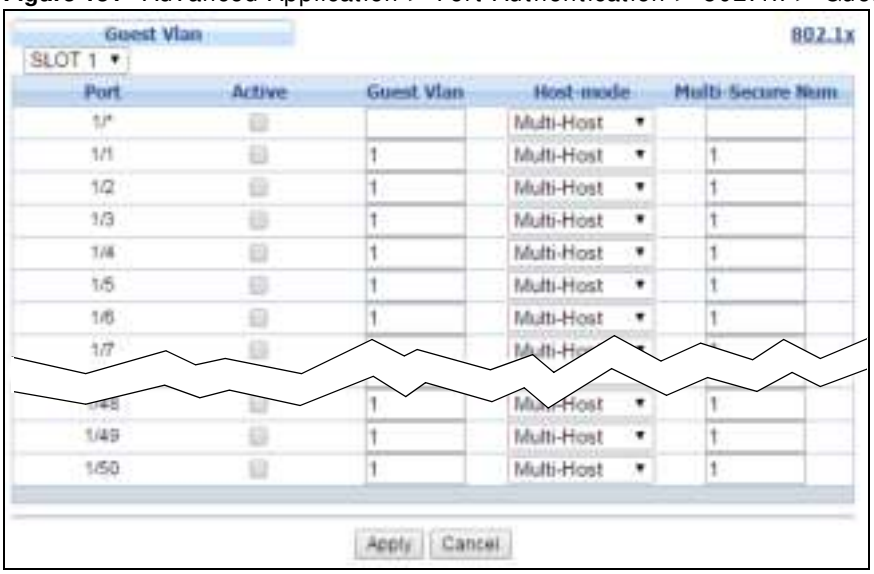


Figure 131 Advanced Application > Port Authentication > 802.1x > Guest VLAN (Stacking mode)



The following table describes the labels in this screen.

Table 80 Advanced Application > Port Authentication > 802.1x > Guest VLAN

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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 checkbox to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.
Guest Vlan	A guest VLAN is a pre-configured VLAN on the Switch that allows non-authenticated users to access limited network resources through the Switch. You must also enable IEEE 802.1x authentication on the Switch and the associated ports. Enter the number that identifies the guest VLAN. Make sure this is a VLAN recognized in your network.
Host-mode	Specify how the Switch authenticates users when more than one user connect to the port (using a hub). Select **Multi-Host** to authenticate only the first user that connects to this port. If the first user enters the correct credential, any other users are allowed to access the port without authentication. If the first user fails to enter the correct credential, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, rest of the users are blocked until a user does the authentication process again. Select **Multi-Secure** to authenticate each user that connects to this port.
Multi-Secure Num	If you set **Host-mode** to **Multi-Secure**, specify the maximum number of users (between 1 and 24) that the Switch will authenticate on this port.

Table 80 Advanced Application > Port Authentication > 802.1x > Guest VLAN (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.2.3 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 132 Advanced Application > Port Authentication > MAC Authentication (Standalone mode)

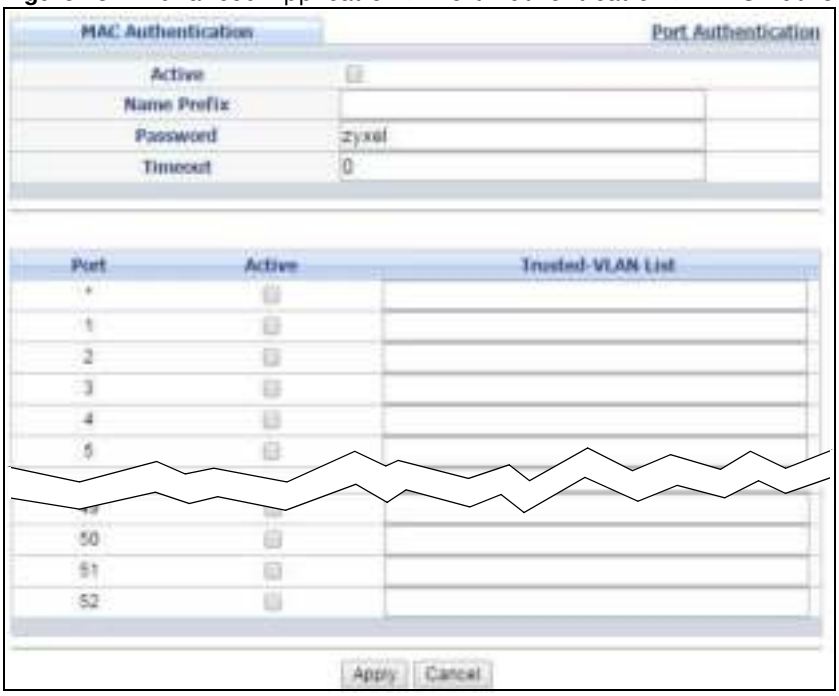
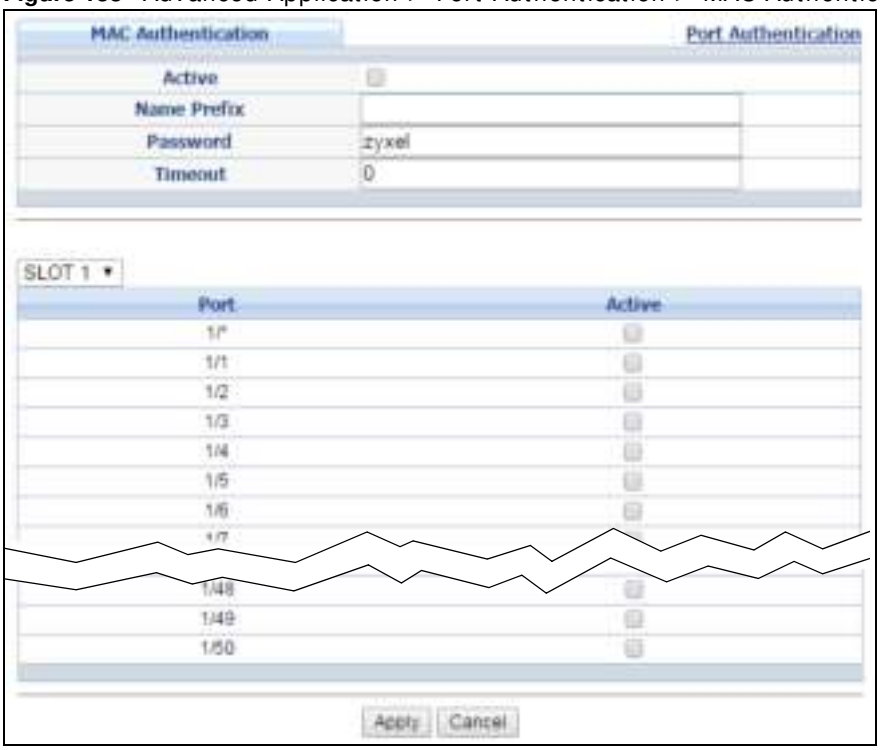


Figure 133 Advanced Application > Port Authentication > MAC Authentication (Stacking mode)



The following table describes the labels in this screen.

Table 81 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.
Timeout	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. 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, the Switch uses the **Aging Time** configured in the **Switch Setup** screen. Note: If the **Aging Time** in the **Switch Setup** screen is set to a lower value, then it supersedes this setting. See Section 6.4 on page 63.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 81 Advanced Application > Port Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
*	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.
Active	Select this check box to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Trusted-VLAN List (Standalone mode)	Enter the ID number(s) of the trusted VLAN(s) (separated by a comma). If a client's VLAN ID is specified here, the client can access the port and the connected networks without MAC authentication.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17

Port Security

This chapter shows you how to set up port security.

17.1 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 32K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 32K.

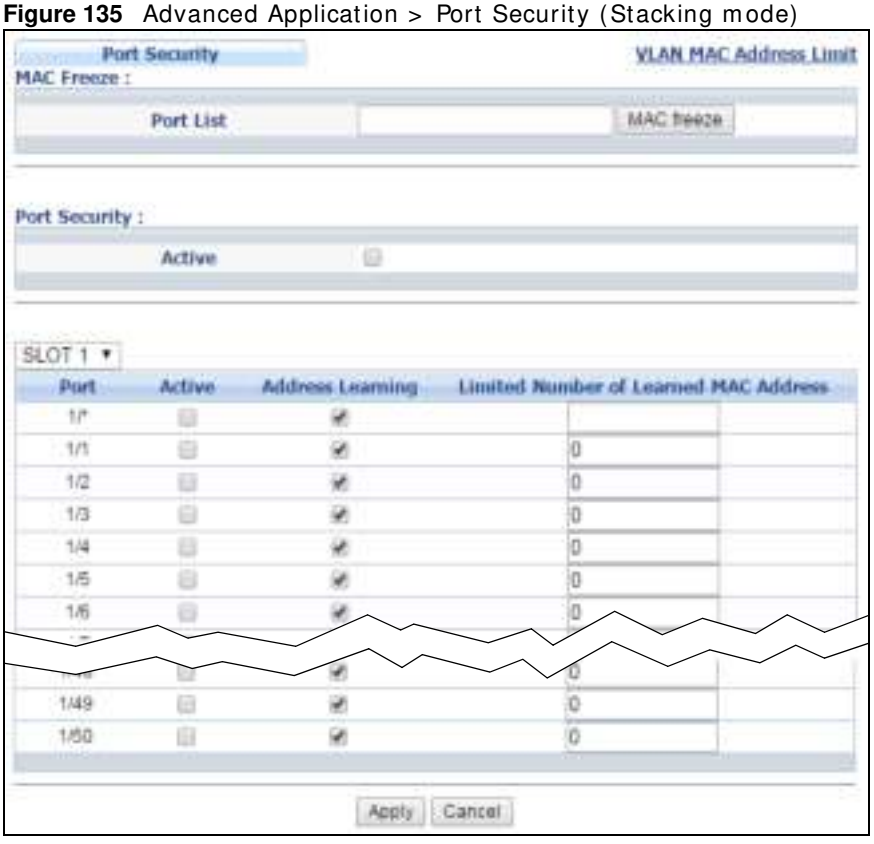
For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

17.2 Port Security Setup

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

Figure 134 Advanced Application > Port Security (Standalone mode)

Figure 135 Advanced Application > Port Security (Stacking mode)



The following table describes the labels in this screen.

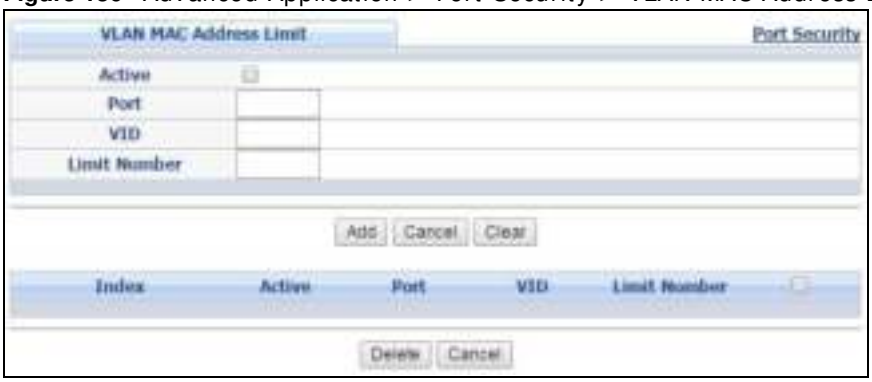
Table 82 Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example. After you click **MAC freeze**, all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the **Static MAC Forwarding** screen.
MAC freeze	Click **MAC freeze** to have the Switch automatically select the **Active** check boxes and clear the **Address Learning** check boxes only for the ports specified in the **Port list**.
Active	Select this option to enable port security on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the 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 the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from “0” to “16K”. “0” means this feature is disabled.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.3 VLAN MAC Address Limit

Use this screen to set the MAC address learning limit on per-port and per-VLAN basis. Click **VLAN MAC Address Limit** in the **Advanced Application > Port Security** screen to display the screen as shown.

Figure 136 Advanced Application > Port Security > VLAN MAC Address Limit



The following table describes the labels in this screen.

Table 83 Advanced Application > Port Security > VLAN MAC Address Limit

LABEL	DESCRIPTION
Active	Select this option to activate this rule.
Port	Enter the number of the port to which this rule is applied. In stacking mode, the first number represents the slot and the second the port number.
VID	Enter the VLAN identification number.
Limit Number	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port in a specified VLAN. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may 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 out time can be set in the **Switch Setup** screen. The valid range is from "0" to "16K". "0" means this feature is disabled.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset 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 **Yes** when the rule is activated and **No** when is it deactivated.
Port	This field displays the number of the port to which this rule is applied.
VID	This is the VLAN ID number to which the port belongs.
Limit Number	This is the maximum number of MAC addresses which a port can learn in a VLAN.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

18

Time Range

This chapter shows you how to set up a time range for time-oriented features on the Switch.

18.1 About Time Range

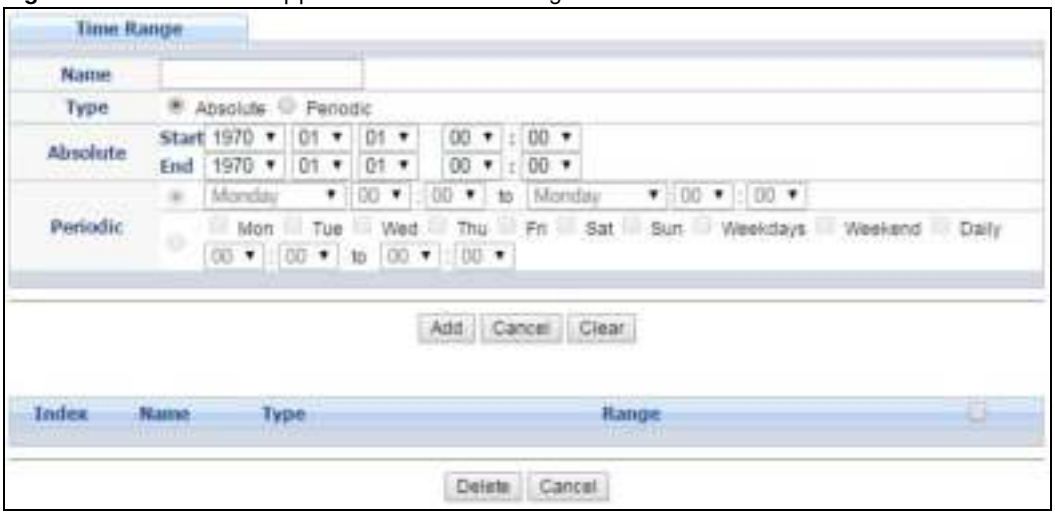
You can set a time range for time-oriented features such as Classifier ACL (Access Control List) rule which categorizes data packets into different network traffic flow. The advantage of the time range feature is that it allows you to schedule the active time of configurations. For example, see Section 19.2 on page 201 to configure the classifier rule with time range.

The time range can be configured in two ways - Absolute and Periodic. Absolute is a fixed time range with a start and end time. Periodic is recurrence of a time range and doesn't have an end time.

18.2 Time Range Setup

Click **Advanced Application** > **Time Range** in the navigation panel to display the screen as shown.

Figure 137 Advanced Application > Time Range



The following table describes the labels in this screen.

Table 84 Advanced Application > Time Range

LABEL	DESCRIPTION
Name	Type a name for this time range rule.
Type	Select a time range type. **Absolute** is a fixed time range that has a set start and end date. **Periodic** is recurrence of a time range.
Absolute	This sets a fixed time range.
Start	Specify the year, month, day, hour and minute when the schedule begins.
End	Specify the year, month, day, hour and minute when the schedule ends.
Periodic	This section is available only when you set **Type** to **Periodic**. Select the first option if you want to define a recurring schedule for a consecutive time period. You then select the day of the week, hour and minute when the schedule begins and ends respectively. Select the second option if you want to define a recurring schedule for multiple non-consecutive time periods. You need to select each day of the week the recurring schedule is effective. You also need to specify the hour and minute when the schedule begins and ends each day. The schedule begins and ends in the same day.
Add	Click **Add** to save the time range you entered.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Name	This field displays the name of the time range rule.
Type	This field displays the type of the schedule.
Range	This field displays the time period(s) to which this schedule applies.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rule(s) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

19

Classifier

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

19.1 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 for a classified traffic flow (refer to Chapter 20 on page 210 to configure policy rules).

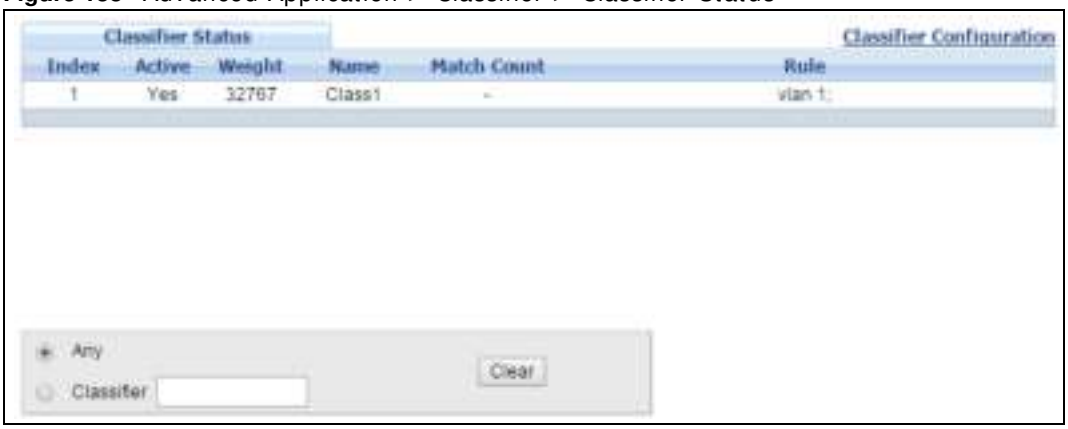
You can also configure policy routing to forward a classified traffic flow to a different gateway for cost savings and load sharing. See Chapter 41 on page 400 for how to configure policy routing.

19.2 Classifier Status

Use this screen to to view the classifiers configured on the Switch and how many times the traffic matches the rules.

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

Figure 138 Advanced Application > Classifier > Classifier Status



The following table describes the labels in this screen.

Table 85 Advanced Application > Classifier > Classifier Status

LABEL	DESCRIPTION
Index	This field displays the index number of the Classifier rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Weight	This field displays the rule's weight. This is to indicate a rule's priority when the match order is set to **manual** in the **Classifier > Classifier Global Setting** screen. The higher the number, the higher the rule's priority.
Name	This field displays the name of the Classifier rule.
Match Count	This field displays the number of times a rule is applied. It displays '-' if the rule does not have count enabled.
Rule	This field displays a summary of the classifier rule's settings.
Any	Select **Any**, then click **Clear** to clear the matched count for all classifiers.
Clear	Select **Classifier**, enter a classifier rule name and then click **Clear** to erase the recorded statistical information for that classifier, or select **Any** to clear statistics for all classifiers.

19.3 Classifier Configuration

Use the **Classifier Configuration** 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. In the **Classifier Status** screen click **Classifier Configuration** to display the configuration screen as shown.

Figure 139 Advanced Application > Classifier > Classifier Configuration

The following table describes the labels in this screen.

Table 86 Advanced Application > Classifier > Classifier Configuration

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.

Table 86 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
Weight	Enter a number between 0 and 65535 to specify the rule's weight. When the match order is in manual mode in the **Classifier Global Setting** screen, a higher weight means a higher priority.
Log	Select this option to have the Switch create a log message when the rule is applied and record the number of matched packets in a particular time interval. Note: Make sure you also enable logging in the **Classifier Global Setting** screen.
Count	Select this option to have the Switch count how many times the rule is applied.
Tme Range	Select the name of the pre-configued schedule that you want to apply to the rule. The rule will be active only at the scheduled date and/or time. If you select **None**, the rule will be active all the time.
Ingress Port	
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (**Any**).
Trunk	Select **Any** to apply the rule to all trunk groups. To specify a trunk group, select the second choice and type a trunk group ID.
Packet Format	Specify the format of the packet. Choices are **All**, **802.3 tagged**, **802.3 untagged**, **Ethernet II tagged** and **Ethernet II untagged**. A value of **802.3** indicates that the packets are formatted according to the IEEE 802.3 standards. A value of **Ethernet II** indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2 Specify the fields below to configure a layer-2 classifier.	
VLAN	
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Inner VLAN	Select **Any** to classify traffic from any inner VLAN (the customer's VLAN) or select the second option and specify the source VLAN ID in the field provided.
Priority	
Priority	Select **Any** to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Inner Priority	Select **Any** to classify traffic from any inner priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select **Others** and enter the Ethernet type number in hexadecimal value. Refer to Table 88 on page 206 for information.
Source	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select **MAC/ Mask** to enter the source MAC address of the packet in valid MAC address format (six hexadecimal character pairs) and type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the **Mask** field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.
Destination	

Table 86 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select **MAC/ Mask** to enter the source MAC address of the packet in valid MAC address format (six hexadecimal character pairs) and type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the **Mask** field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.
Layer 3 Specify the fields below to configure a layer-3 classifier.	
IP Packet Length	Click **Any** to classify any size of packet length or manually enter a range of number (from/to) of packet size in the field provided.
DSCP IPv4/ IPv6	Select **Any** 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.
Precedence	Select **Any** to classify traffic from any precedence or select the second option and specify an IP Precedence (the first 3 bits of of the 8-bit ToS field) value between 0 and 7 in the field provided.
ToS	Select **Any** to classify traffic from any ToS or select the second option and specify Type of Service (the last 5 bits of the 8-bit ToS field) value between 0 and 255 in the field provided.
IP Protocol	Select an IPv4 protocol type or select **Other** and enter the protocol number in decimal value. Refer to Table 89 on page 207 for more information. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
IPv6 Next Header	Select an IPv6 protocol type or select **Other** and enter an 8-bit next header in the IPv6 packet. The Next Header field is similar to the IPv4 Protocol field. The IPv6 protocol number ranges from 1 to 255. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
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.
Destination	
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.
Layer 4 Specify the fields below to configure a layer-3 classifier.	
Source/ Destination Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.

Table 86 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.

19.3.1 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 a lower layer rule.

Figure 140 Advanced Application > Classifier > Classifier Configuration: Summary Table

The following table describes the labels in this screen.

Table 87 Advanced Application > Classifier > Classifier Configuration: 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 **Yes** when the rule is activated and **No** when it is deactivated.
Weight	The field displays the priority of the rule when the match order is in **manual** mode. A higher weight means a higher priority.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
Rule	This field displays a summary of the classifier rule's settings.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 88 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804

Table 88 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

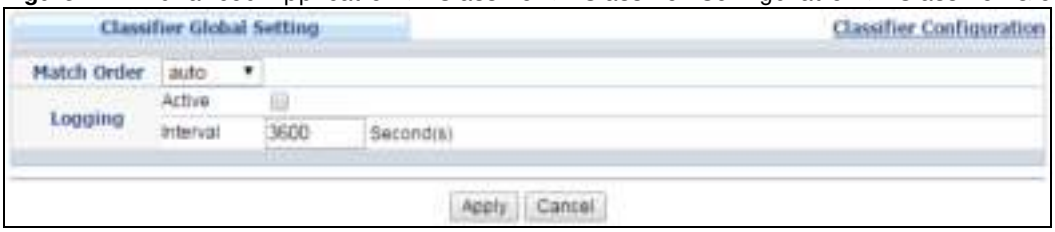
Table 89 Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

19.4 Classifier Global Setting Configuration

Use this screen to configure the match order and enable logging on the Switch. In the **Classifier Configuration** screen click **Classifier Global Setting** to display the configuration screen as shown.

Figure 141 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting



The following table describes the labels in this screen.

Table 90 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting

LABEL	DESCRIPTION
Match Order	Select **manual** to have classifier rules applied according to the weight of each rule you configured in **Advanced Application > Classifier > Classifier Configuration**. Alternatively, select **auto** to have classifier rules applied according to the layer of the item configured in the rule. Layer-4 items have the highest priority, and layer-2 items has the lowest priority. For example, you configure a layer-2 item (VLAN ID) in classifier A and configure a layer-3 item (source IP address) in classifier B. When an incoming packet matches both classifier rules, classifier B has priority over classifer A.
Logging	

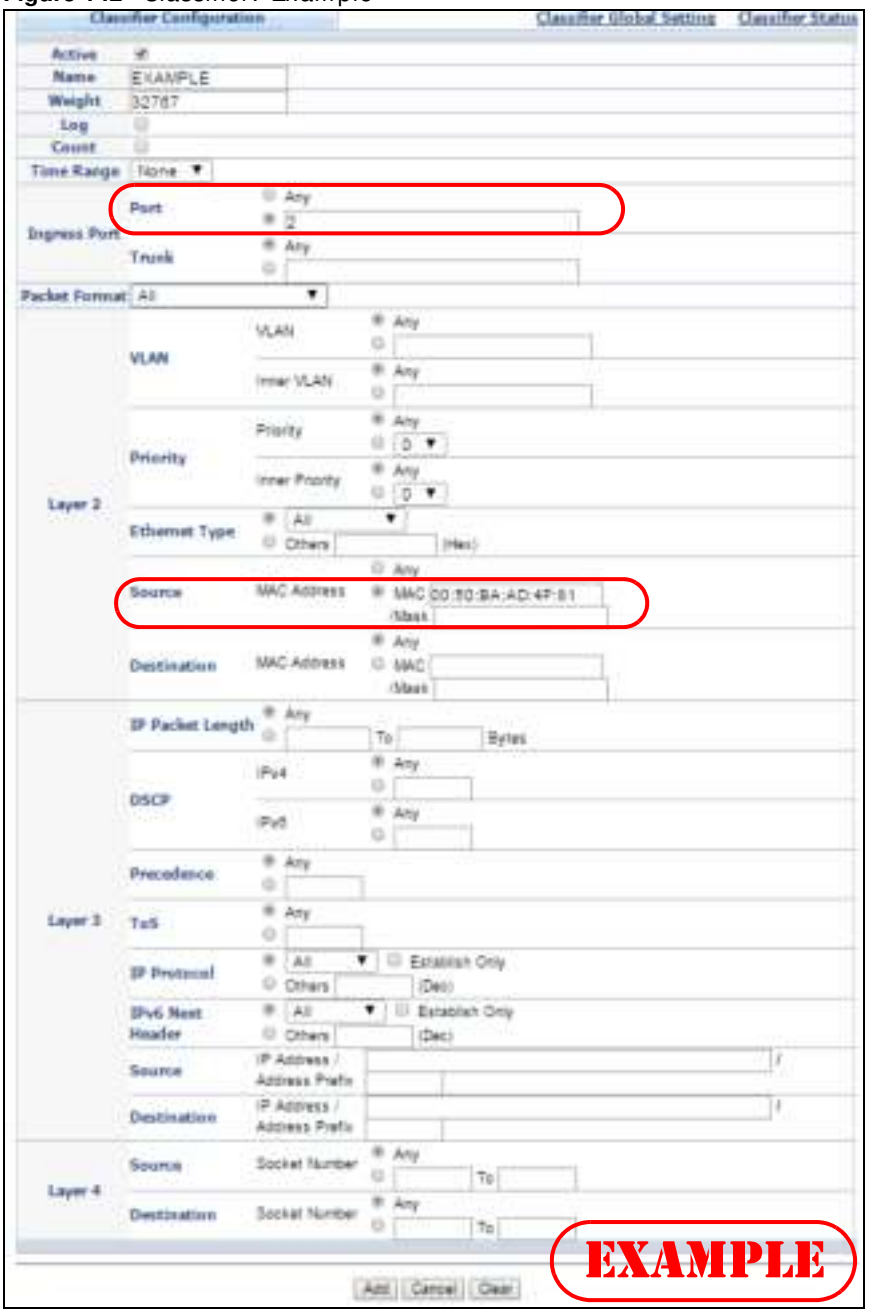
Table 90 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting

LABEL	DESCRIPTION
Active	Select this to allow the Switch to create a log when packets match a classifier rule during a defined time interval.
Interval	Select the length of the time period (in seconds) to count matched packets for a classifier rule. Enter an integer from 0-65535. 0 means that no logging is done.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19.5 Classifier Example

The following screen shows an example of configuring a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

Figure 142 Classifier: Example



After you have configured a classifier, you can configure a policy to define action(s) on the classified traffic flow. See Chapter 20 on page 210 for information on configuring a policy rule.

20

Policy Rule

This chapter shows you how to configure policy rules.

20.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 19 on page 201 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

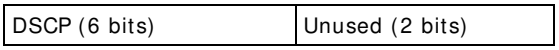
20.1.1 DiffServ

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.

20.1.2 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.



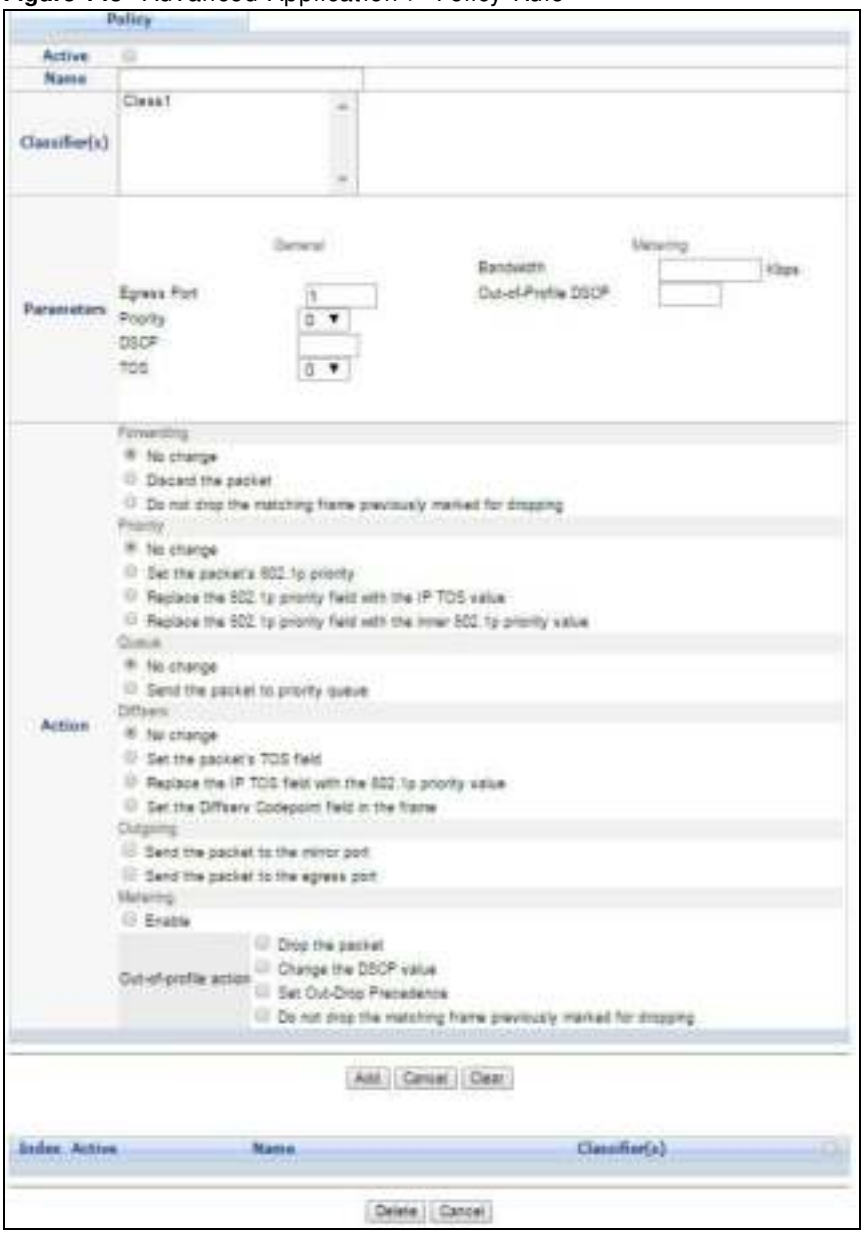
The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

20.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to Section 19.2 on page 201 for more information.

Click **Advanced Application > Policy Rule** in the navigation panel to display the screen as shown.

Figure 143 Advanced Application > Policy Rule



The following table describes the labels in this screen.

Table 91 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 **Classifier** 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.

Table 91 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
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 **Action** field.	
General	
Egress Port	Type the number of an outgoing port. In stacking mode, the first number represents the slot and the second the port number.
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 **No change** to forward the packets. Select **Discard the packet** to drop the packets. Select **Do not drop the matching frame previously marked for dropping** to retain the frames that were marked to be dropped before.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1p priority** to replace the packet's 802.1p priority field with the value you set in the **Priority** field. Select **Replace the 802.1p priority field with the IP TOS value** to replace the packet's 802.1p priority field with the value you set in the **TOS** field. Select **Replace the 802.1p priority field with the inner 802.1p priority value** to replace the packet's 802.1p priority field with the existing customer priority level carried in the frames.
Queue	Select **No change** to keep the priority setting of the frames. Select **Send the packet to priority queue** to replace the packet's 802.1p priority field with the value you set in the **Priority** field. Note: If you select **Send the packet to priority queue**, the system will automatically select other options except for the **No change** in the **Priority** field.
Diffserv	Select **No change** to keep the TOS and/or DSCP fields in the packets. Select **Set the packet's TOS field** to set the TOS field with the value you configure in the **TOS** field. Select **Replace the IP TOS with the 802.1p priority value** to replace the TOS field with the value you configure in the **Priority** field. Select **Set the Diffserv Codepoint field in the frame** to set the DSCP field with the value you configure in the **DSCP** field.
Outgoing	Select **Send the packet to the mirror port** to send the packet to the mirror port. Select **Send the packet to the egress port** to send the packet to the egress port.

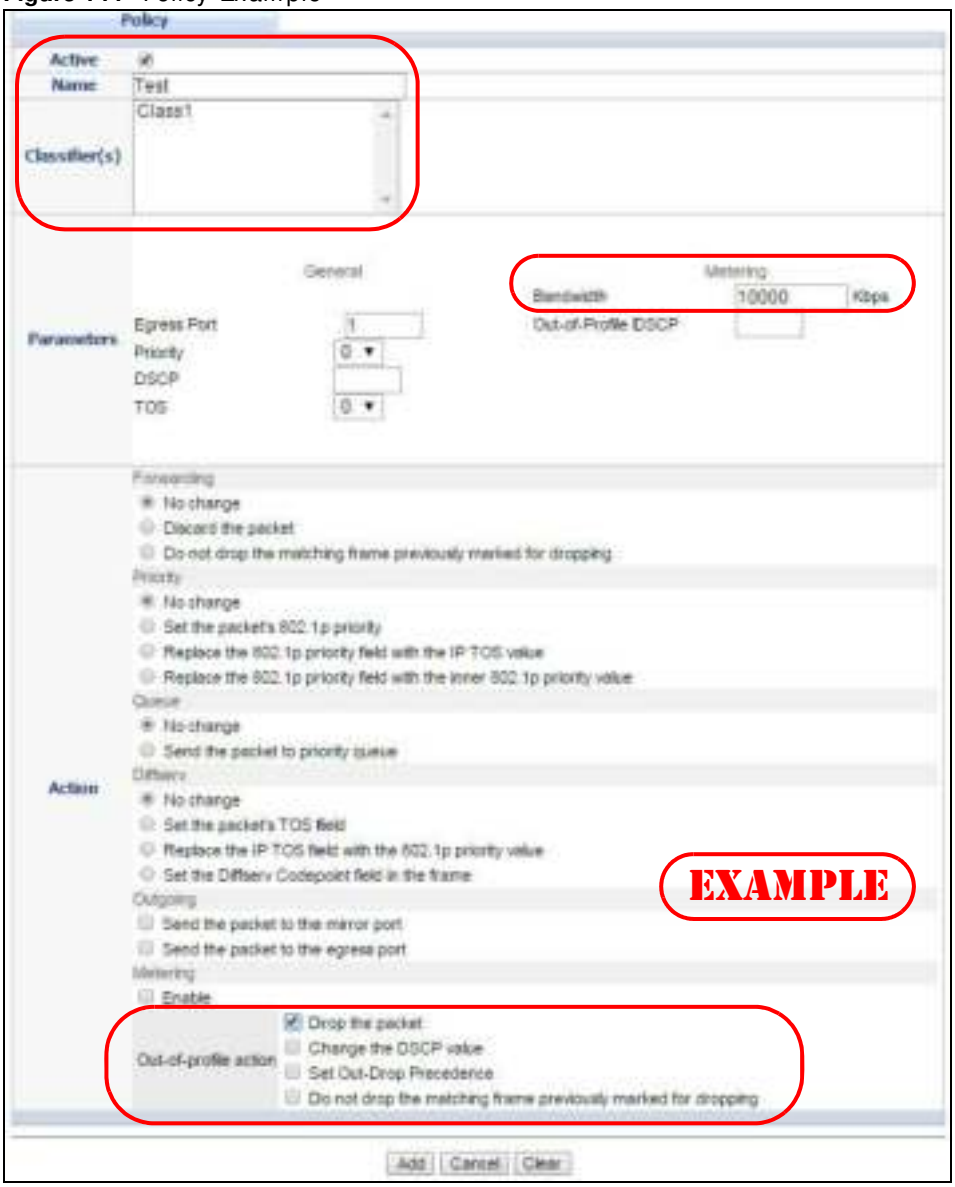
Table 91 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Metering	Select **Enable** to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select **Drop the packet** to discard the out-of-profile traffic. Select **Change the DSCP value** to replace the DSCP field with the value specified in the **Out of profile DSCP** field. Select **Set Out-Drop Precedence** to mark out-of-profile traffic and drop it when network is congested. Select **Do not drop the matching frame previously marked for dropping** to queue the frames that are marked to be dropped.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays **Yes** when policy is activated and **No** when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

20.3 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 19.5 on page 208).

Figure 144 Policy Example



21

Queuing Method

This chapter introduces the queuing methods supported.

21.1 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.

21.1.1 Strictly Priority

Strictly Priority (SP) 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.

21.1.2 Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (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. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

The weights range from 1 to 15 and the actual guaranteed bandwidth is calculated as follows:

Weight x 2 KB

If the weight setting is 5, the actual quantum guaranteed to the associated queue would be as follows:

5 x 2KB = 10 KB

21.1.3 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.

21.2 Configuring Queuing

Click **Advanced Application** > **Queuing Method** in the navigation panel.

Figure 145 Advanced Application > Queuing Method (Standalone mode)

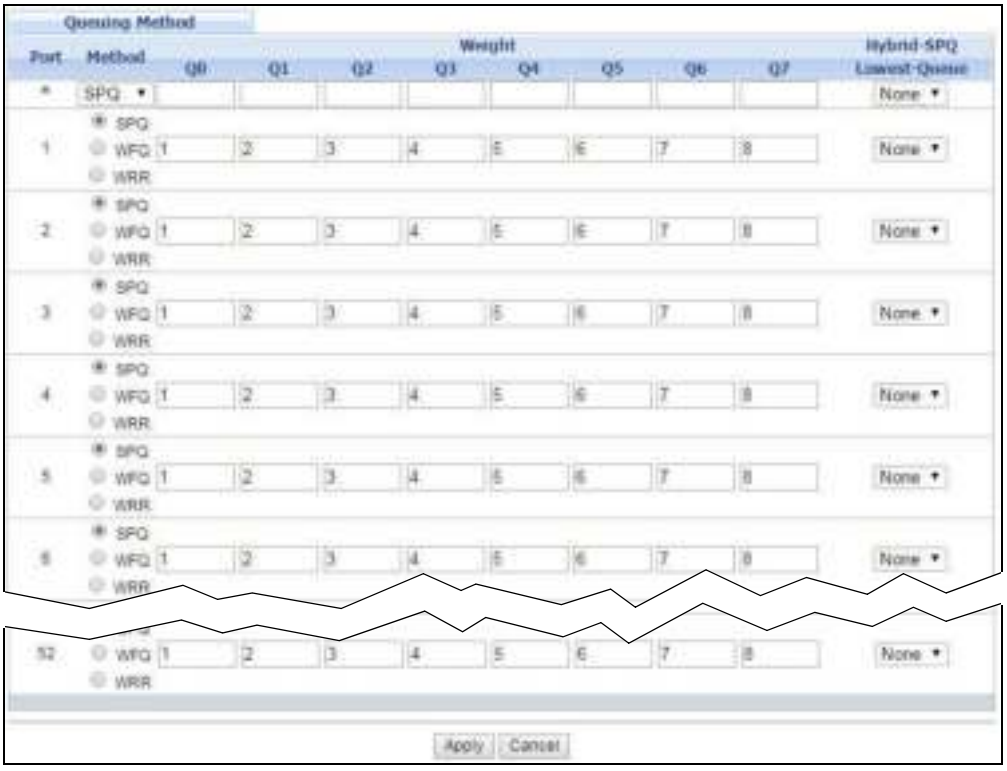
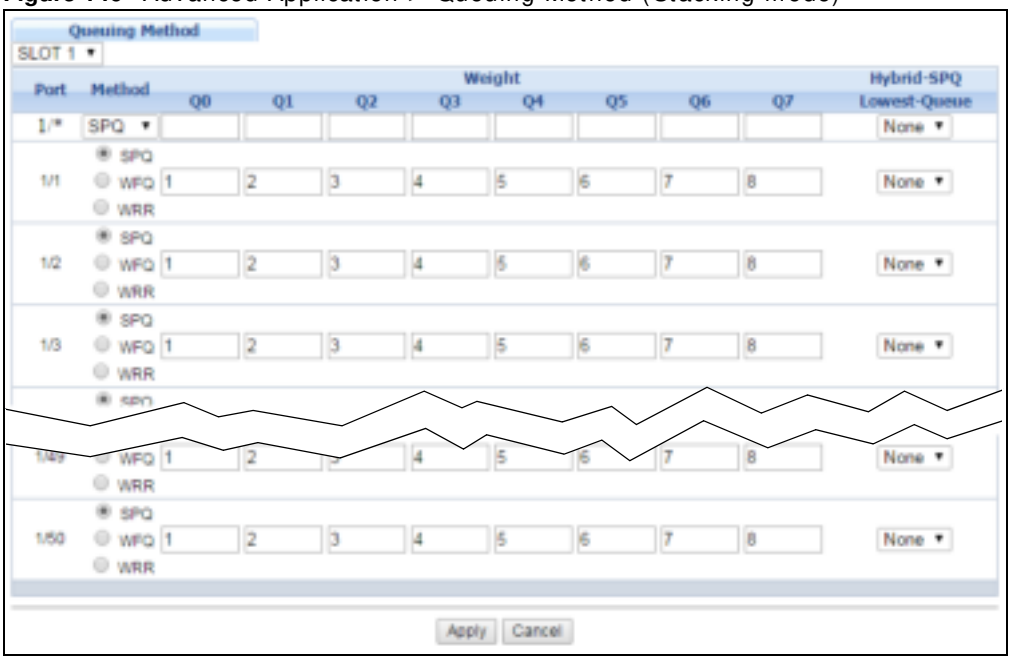


Figure 146 Advanced Application > Queuing Method (Stacking mode)



The following table describes the labels in this screen.

Table 92 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Method	Select **SPQ** (Strictly Priority Queuing), **WFQ** (Weighted Fair Queuing) or **WRR** (Weighted Round Robin). 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. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth weight (the number you configure in the **Weight** field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Weight Q0-Q7	When you select **WFQ** or **WRR** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.

Table 92 Advanced Application > Queuing Method (continued)

LABEL	DESCRIPTION
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select **WFQ** or **WRR**. Select a queue (**Q0** to **Q7**) to have the Switch use **SPQ** to service the subsequent queue(s) after and including the specified queue for the 1000Base-T, 1000Base-X and 10 Gigabit Ethernet ports. For example, if you select **Q5**, the Switch services traffic on **Q5**, **Q6** and **Q7** using **SPQ**. Select **None** to always use **WFQ** or **WRR**.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

22

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

22.1 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.

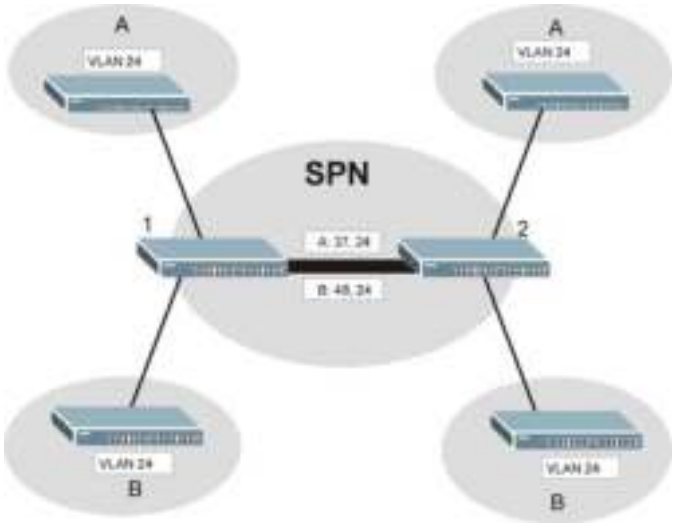
Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider 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.

22.1.1 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 147 VLAN Stacking Example



22.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel Port** (the latter is for Gigabit ports only).

- 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 the Service Provider’s (SP) VLAN ID (VID)).

Note: Static VLAN **Tx Tagging** MUST be enabled on a port where you choose **Tunnel Port**.

22.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 93 VLAN Tag Format

Type	Priority	VID

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the Switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel Port**, then the Switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the Switch. (If an incoming frame's **SP TPID** is the same as the one configured on the Switch, then the Switch will not add the tag.)

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 the 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.

22.3.1 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 94 Single and Double Tagged 802.1Q Frame Format

						DA	SA	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	**TPID**	**Priority**	**VID**	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	**SPTPID**	**Priority**	**VID**	**TPID**	**Priority**	**VID**	Len/Etype	Data	FCS	Double-tagged frame

Table 95 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

22.4 Configuring VLAN Stacking

Click **Advanced Application > VLAN Stacking** to display the screen as shown.

Figure 148 Advanced Application > VLAN Stacking (Standalone mode)

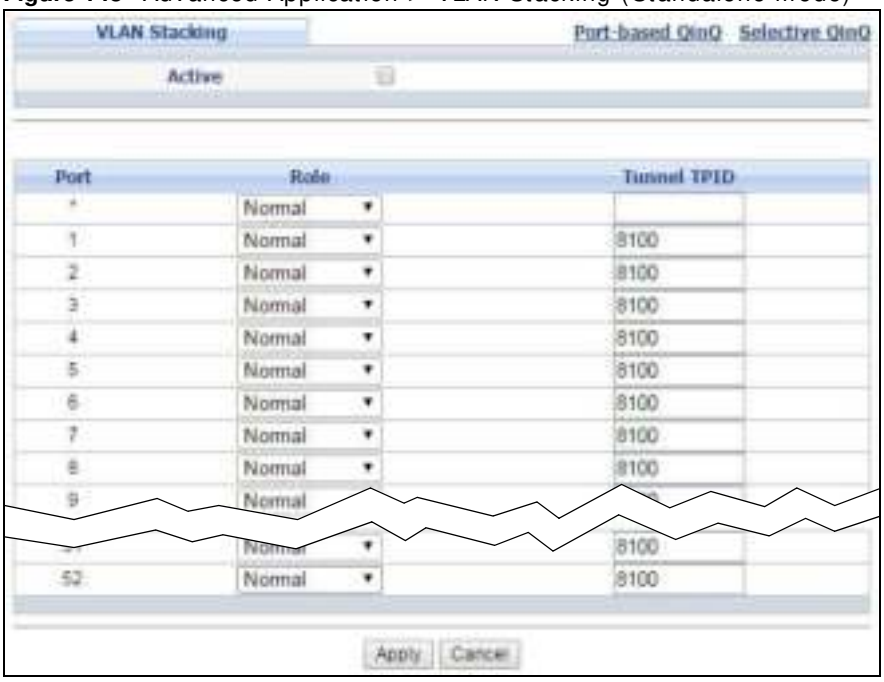
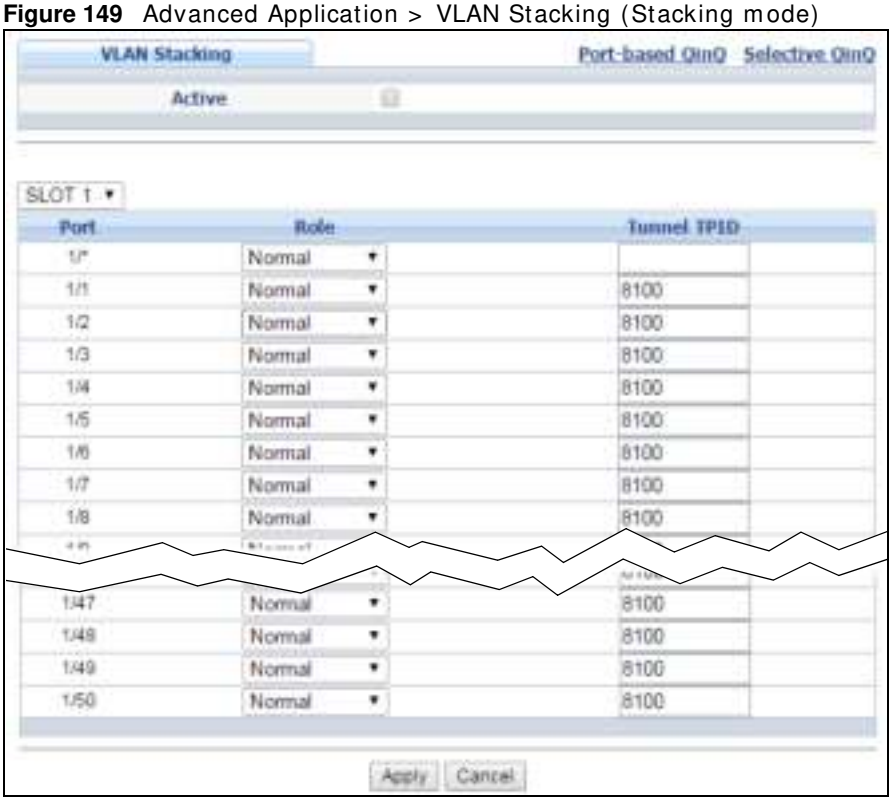


Figure 149 Advanced Application > VLAN Stacking (Stacking mode)



The following table describes the labels in this screen.

Table 96 Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Role	Select **Normal** to have the Switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in **SPVID** and **Priority** of the **Port-based QinQ** or the **Selective QinQ** screen are ignored. Select **Access Port** to have the Switch add the SP TPID tag to all incoming frames received on this port. Select **Access Port** for ingress ports at the edge of the service provider's network. Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. Select **Tunnel Port** to have the Switch add the **Tunnel TPID** tag to all outgoing frames sent on this port. 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.
Tunnel TPID	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. 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. Note: You can define up to four different tunnel TPIDs (including **8100**) in this screen at a time.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

22.4.1 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 150 Advanced Application > VLAN Stacking > Port-based QinQ (Standalone mode)

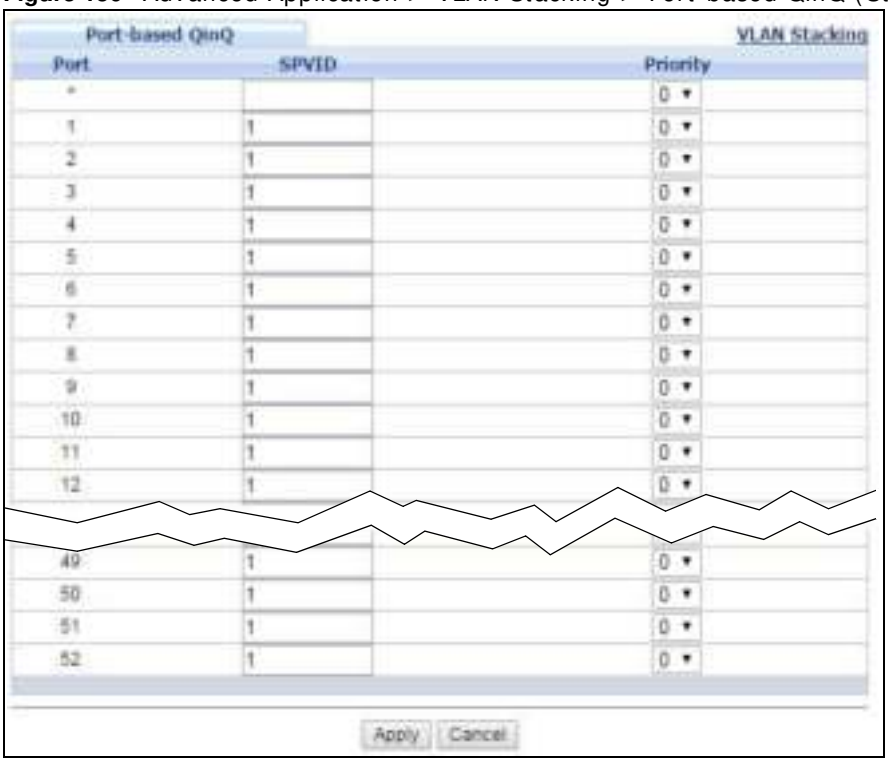
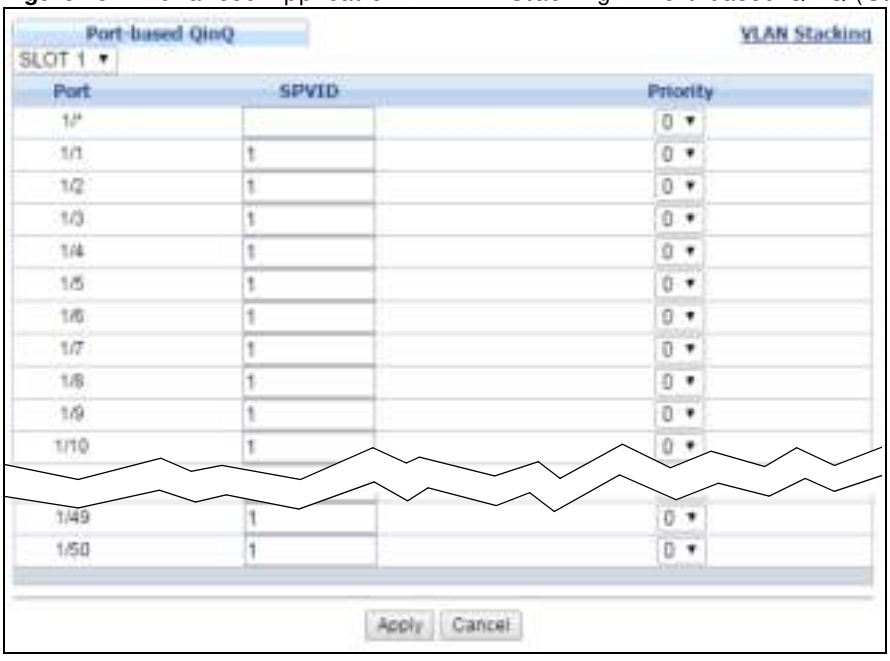


Figure 151 Advanced Application > VLAN Stacking > Port-based QinQ (Stacking mode)



The following table describes the labels in this screen.

Table 97 Advanced Application > VLAN Stacking > Port-based QinQ

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
SPVID	**SPVID** 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 Chapter 7 on page 101 for more background information on VLAN ID.
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. "0" is the lowest priority level and "7" is the highest.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

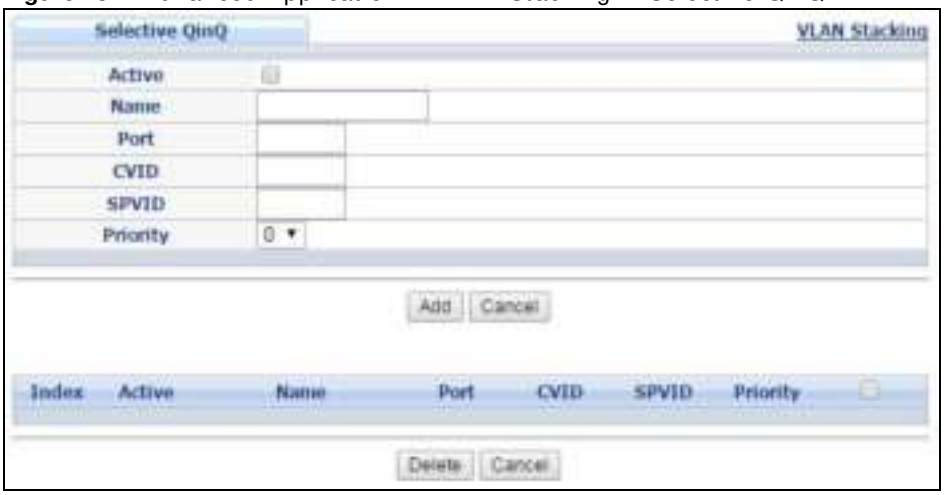
22.4.2 Selective Q-in-Q

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 152 Advanced Application > VLAN Stacking > Selective QinQ



The following table describes the labels in this screen.

Table 98 Advanced Application > 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. In stacking mode, the first field is the slot ID and the second field is the port number.
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	**SPVID** 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 Chapter 7 on page 101 for more background information on VLAN ID.
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. "0" is the lowest priority level and "7" is the highest.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the number of the selective VLAN stacking rule. Click on an index number to change the settings.
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. In stacking mode, the first number represents the slot and the second the port number.
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.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

23

Multicast

This chapter shows you how to configure various multicast features.

23.1 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 an IPv4 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.

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 similar to IGMPv2 and MLDv2 is similar to IGMPv3. MLD allows an IPv6 switch or router to discover the presence of MLD listeners 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.

23.1.1 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 website for more information).

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group. Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8.

23.1.2 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.

23.1.3 IGMP Snooping

The 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.

23.1.4 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.

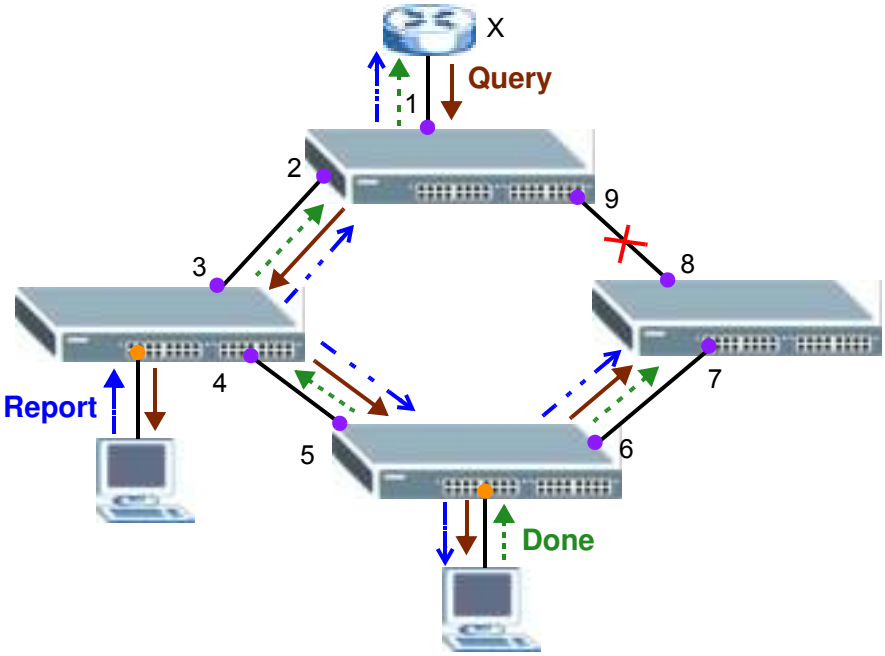
23.1.5 MLD Snooping-Proxy

MLD snooping-proxy is a ZyXEL-proprietary feature. IPv6 MLD proxy allows only one upstream interface on a switch, while MLD snooping-proxy supports more than one upstream port on a switch. The upstream port in MLD snooping-proxy can report group changes to a connected multicast router and forward MLD messages to other upstream ports. This helps especially when you want to have a network that uses STP to provide backup links between switches and also performs MLD snooping and proxy functions. MLD snooping-proxy, like MLD proxy, can minimize MLD control messages and allow better network performance.

In MLD snooping-proxy, if one upstream port is learned via snooping, all other upstream ports on the same device will be added to the same group. If one upstream port requests to leave a group, all other upstream ports on the same device will also be removed from the group.

In the following MLD snooping-proxy example, all connected upstream ports (1 ~ 7) are treated as one interface. The connection between ports 8 and 9 is blocked by STP to break the loop. If there is

one query from a router (**X**) or MLD Done or Report message from any upstream port, it will be broadcast to all connected upstream ports.



23.1.6 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 similar 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.

23.2 Multicast Setup

Use this screen to configure IGMP for IPv4 or MLD for IPv6 and set up multicast VLANs. Click **Advanced Application** > **Multicast** in the navigation panel.

Figure 153 Advanced Application > Multicast Setup

The following table describes the labels in this screen.

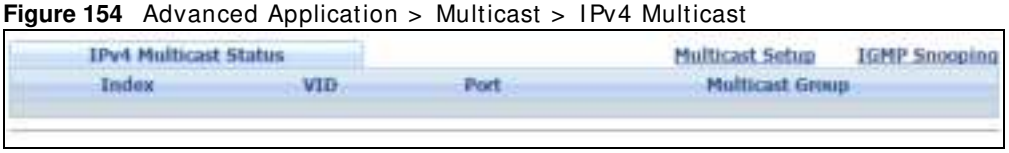
Table 99 Advanced Application > Multicast Setup

LABEL	DESCRIPTION
IPv4 Multicast	Click the link to open screens where you can configure IGMP snooping and IGMP filtering for IPv4.
IPv6 Multicast	Click the link to open screens where you can configure MLD snooping and MLD filtering for IPv6.
MVR	Click the link to open screens where you can create multicast VLANs.

23.3 IPv4 Multicast Status

Click **Advanced Application > Multicast > IPv4 Multicast** to display the screen as shown. This screen shows the IPv4 multicast group information. See Section 23.1 on page 227 for more information on multicasting.

Figure 154 Advanced Application > Multicast > IPv4 Multicast



The following table describes the labels in this screen.

Table 100 Advanced Application > Multicast > IPv4 Multicast

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group. In stacking mode, the first number represents the slot and the second the port number.
Multicast Group	This field displays IP multicast group addresses.

23.3.1 IGMP Snooping

Click the **IGMP Snooping** link in the **Advanced Application > Multicast > IPv4 Multicast** screen to display the screen as shown. See Section 23.1 on page 227 for more information on multicasting.

Figure 155 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (Standalone mode)

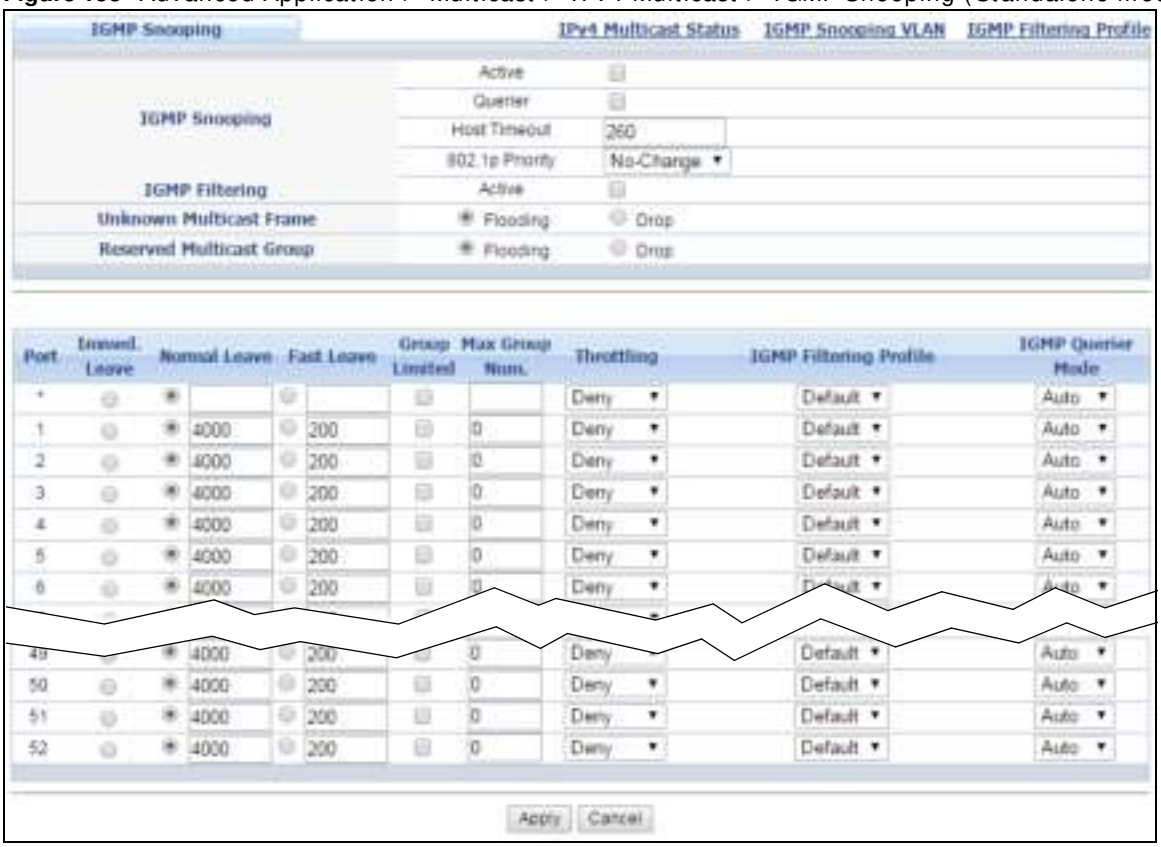
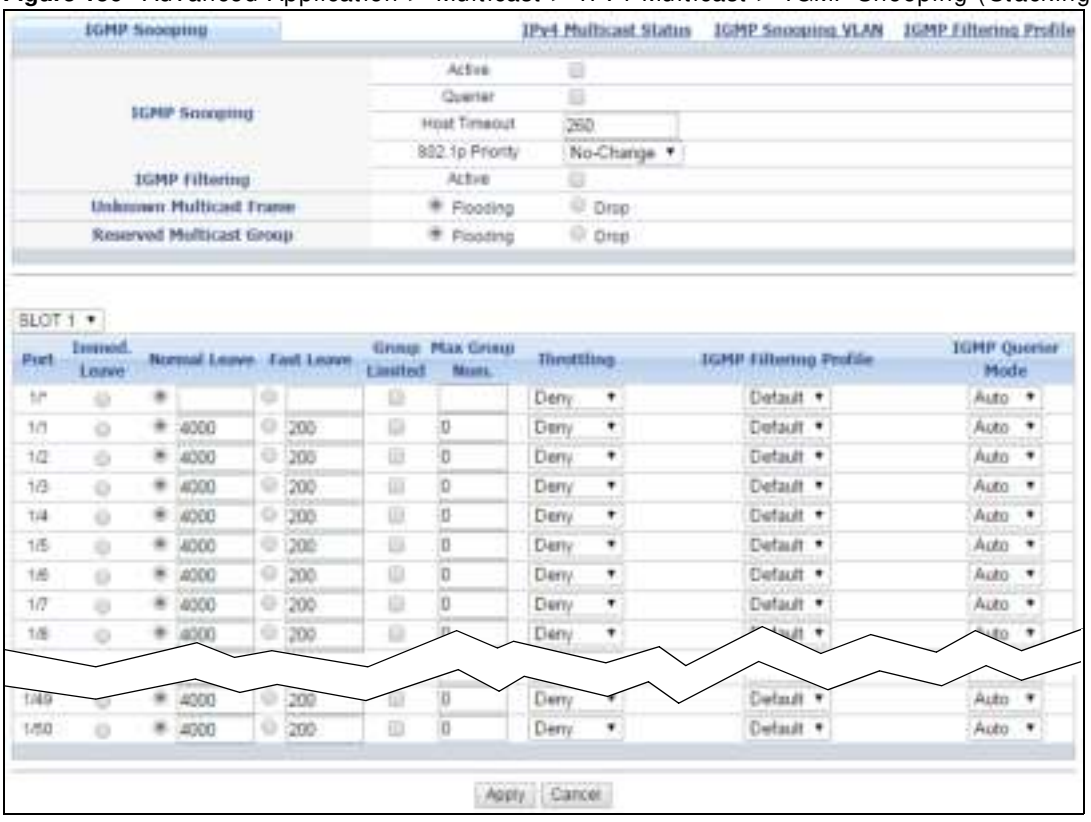


Figure 156 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (Stacking mode)



The following table describes the labels in this screen.

Table 101 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP snooping.
Active	Select **Active** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
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.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. 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.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first field is the slot ID and the second field is 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.
Immed. Leave	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. Select this option if there is only one host connected to this port.

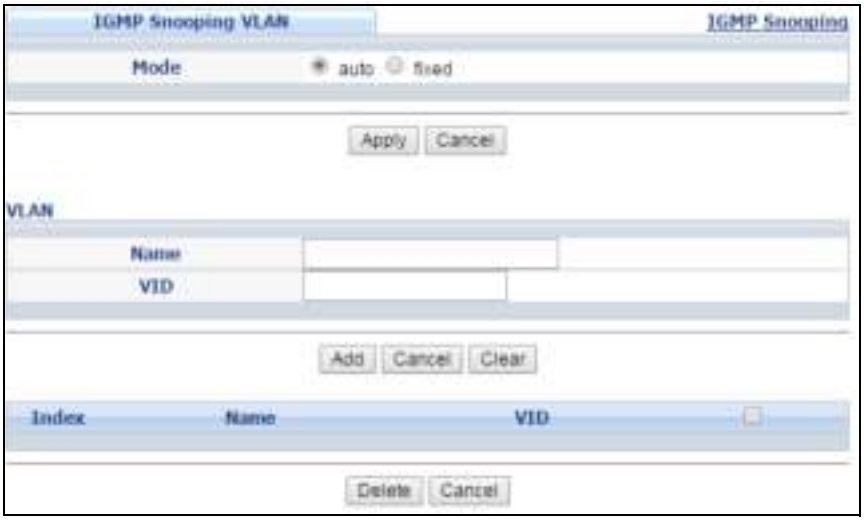
Table 101 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In normal leave mode, when the Switch receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. 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 on this port from a host.
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In fast leave mode, right after receiving an IGMP leave message from a host on a port, the Switch itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process. 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 on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter 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.
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select **Deny** to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select **Replace** to replace an existing entry in the multicast forwarding table with the new IGMP report(s) received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the **Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile** screen.
IGMP Querier Mode	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. Select **Auto** to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** 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. Select **Edge** 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.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.3.2 IGMP Snooping VLAN

Click **Advanced Application > Multicast > IPv4 Multicast** in the navigation panel. Click the **IGMP Snooping** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See Section 23.1.4 on page 228 for more information on IGMP Snooping VLAN.

Figure 157 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN



The following table describes the labels in this screen.

Table 102 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs (including up to five VLANs you configured in the **MVR** screen). For example, if you have configured one multicast VLAN in the **MVR** screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. Note: You must also enable IGMP snooping in the **Multicast > IPv4 Multicast > IGMP Snooping** screen first.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** 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 **MVR** screen.

Table 102 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN (continued)

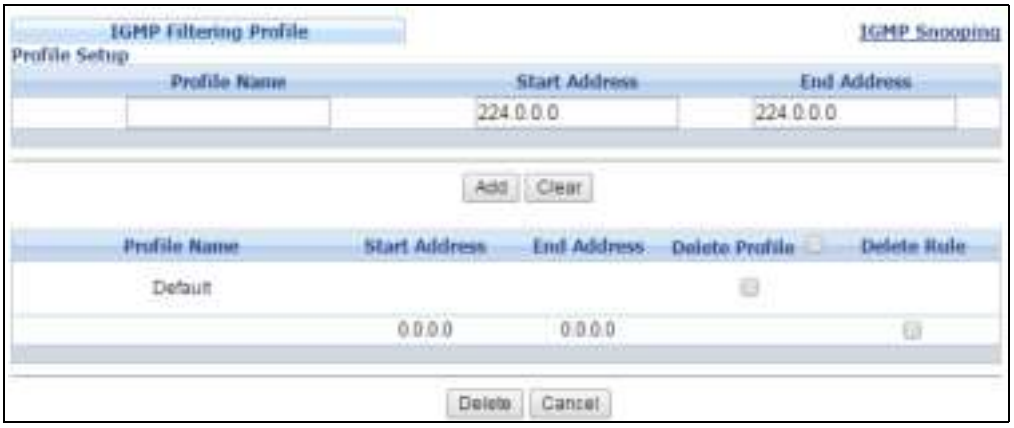
LABEL	DESCRIPTION
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the index 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.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove, then click the **Delete** button.
Cancel	Click **Cancel** to clear the check boxes.

23.3.3 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 **IGMP Snooping** 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 > IPv4 Multicast** in the navigation panel. Click the **IGMP Snooping** link and then the **IGMP Filtering Profile** link to display the screen as shown.

Figure 158 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile



The following table describes the labels in this screen.

Table 103 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > 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 IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP 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 **Start Address** and **End Address** fields.
Add	Click this to create a new entry. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to reset 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 Profile	Select a profile's check box to select a specific profile. Otherwise, select the check box in the table heading row to select all profiles.
Delete Rule	Select the check box(es) of the rule(s) that you want to remove from a profile.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

23.4 IPv6 Multicast Status

Click **Advanced Application > Multicast > IPv6 Multicast** to display the screen as shown. This screen shows the IPv6 multicast group information. See Section 23.1 on page 227 for more information on multicasting.

Figure 159 Advanced Application > Multicast > IPv6 Multicast

The following table describes the labels in this screen.

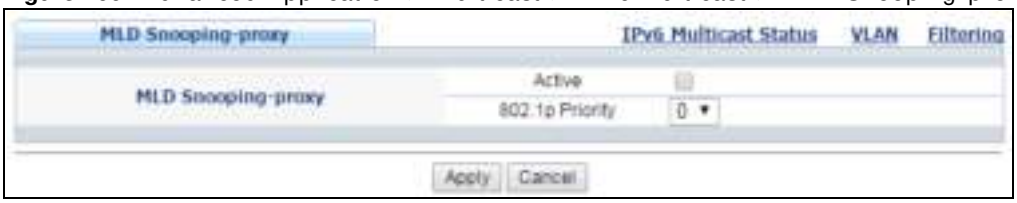
Table 104 Advanced Application > Multicast > IPv6 Multicast

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group. In stacking mode, the first number represents the slot and the second the port number.
Multicast Group	This field displays IP multicast group addresses.
Group Timeout	This field displays the time (in seconds) that elapses before the Switch removes an MLD group membership entry if it does not receive report messages from the port.

23.4.1 MLD Snooping-proxy

Click the **MLD Snooping-proxy** link in the **Advanced Application > Multicast > IPv6 Multicast** screen to display the screen as shown. See Section 23.1 on page 227 for more information on multicasting.

Figure 160 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy



The following table describes the labels in this screen.

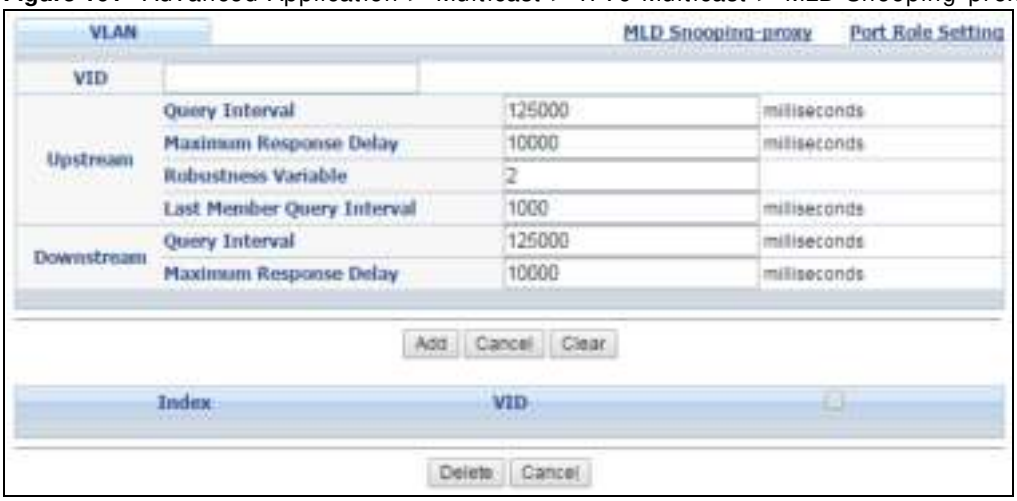
Table 105 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy

LABEL	DESCRIPTION
MLD Snooping-proxy	Use these settings to configure MLD snooping-proxy.
Active	Select **Active** to enable MLD snooping-proxy on the Switch to minimize MLD control messages and allow better network performance.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing MLD messages.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.4.2 MLD Snooping-proxy VLAN

Click the **MLD Snooping-proxy** link and then the **VLAN** link in the **Advanced Application > Multicast > IPv6 Multicast** screen to display the screen as shown. See Section 23.1 on page 227 for more information on multicasting.

Figure 161 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN



The following table describes the labels in this screen.

Table 106 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN on which you want to enable MLD snooping-proxy and configure related settings.
Upstream	
Query Interval	Enter the amount of time (in miliseconds) between general query messages sent by the router connected to the upstream port. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be T = (QI*RV) + MRD, where T = Timeout, QI = Query Interval, RV = Robustness Variable, and MRD = Maximum Response Delay.
Maximum Response Delay	Enter the amount of time (in miliseconds) the router connected to the upstream port waits for a response to an MLD general query message. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be T = (QI*RV) + MRD, where T = Timeout, QI = Query Interval, RV = Robustness Variable, and MRD = Maximum Response Delay. When an MLD Done message is received, the Switch sets the entry's lifetime to be the product of **Last Member Query Interval** and **Robustness Variable**
Robustness Variable	Enter the number of queries. A multicast address entry (learned only on an upstream port by snooping) is removed from the forwarding table when there is no response to the configured number of queries sent by the router connected to the upstream port. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table.

Table 106 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

LABEL	DESCRIPTION
Last Member Query Interval	Enter the amount of time (in miliseconds) between the MLD group-specific queries sent by an upstream port when an MLD Done message is received. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table after a Done message is received. When an MLD Done message is received, the Switch sets the entry's lifetime to be the product of **Last Member Query Interval** and **Robustness Variable**.
Downstream	
Query Interval	Enter the amount of time (in miliseconds) between general query messages sent by the downstream port.
Maximum Response Delay	Enter the maximum time (in miliseconds) that the Switch waits for a response to a general query message sent by the downstream port.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the index number of the MLD snooping-proxy VLAN entry in the table. Click on an index number to view more details or change the settings.
VID	This field displays the ID number of the VLAN group.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry(ies) permanently.
Cancel	Click **Cancel** to clear the check boxes.

23.4.3 MLD Snooping-proxy VLAN Port Role Setting

Click the **Port Role Setting** link in the **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN** screen to display the screen as shown. See Section 23.1 on page 227 for more information on multicasting.

Figure 162 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting (Standalone mode)

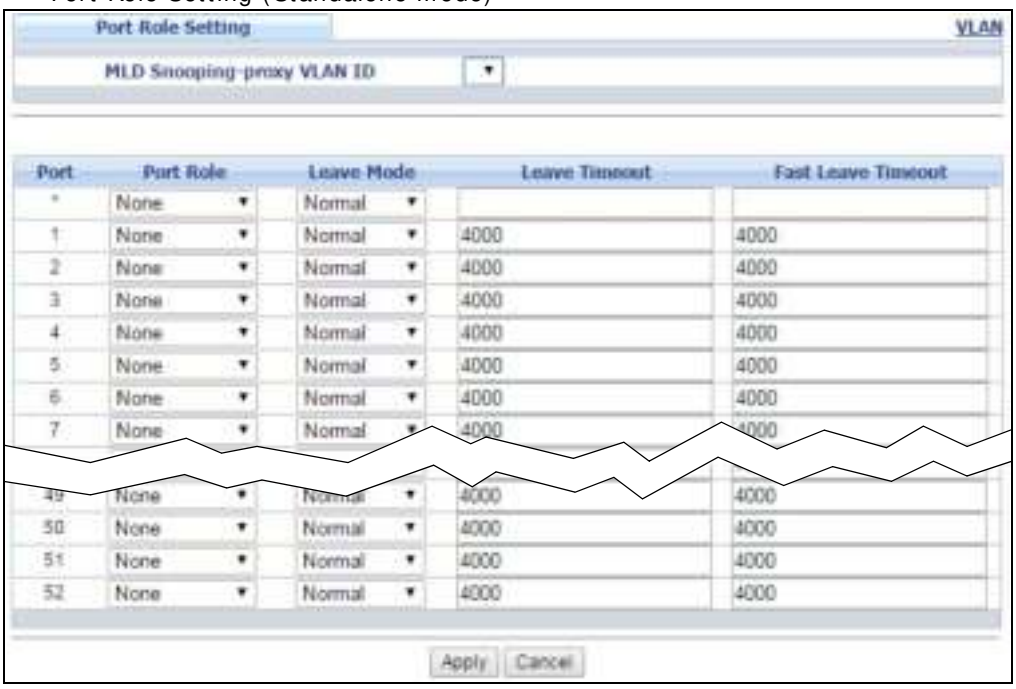
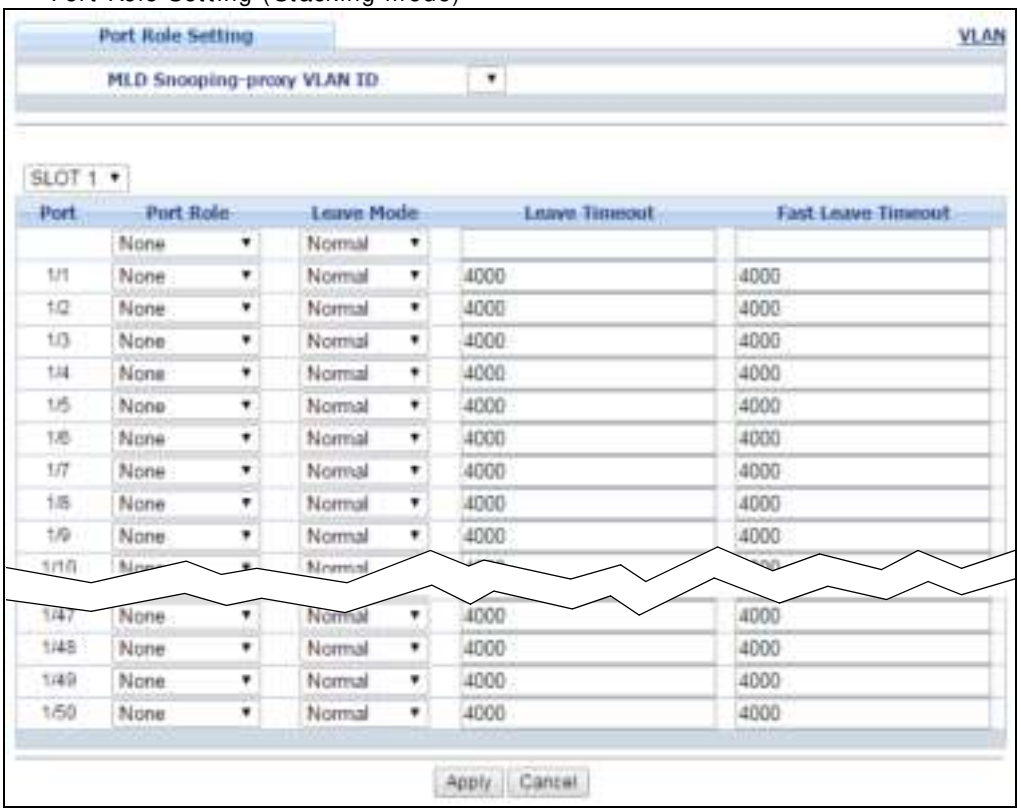


Figure 163 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting (Stacking mode)



The following table describes the labels in this screen.

Table 107 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting

LABEL	DESCRIPTION
MLD Snooping-proxy VLAN ID	Select the VLAN ID for which you want to configure a port's MLD snooping-proxy settings.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Port Role	A port on the Switch can be either a **Downstream** port or **Upstream** port in MLD. A downstream port connects to MLD hosts and acts as a multicast router to send MLD queries and listen to the MLD host's Report and Done messages. An upstream port connects to a multicast router and works as a host to send Report or Done messages when receiving queries from a multicast router. Otherwise, select **None** if the port is not joining a multicast group or does not belong to this VLAN.
Leave Mode	Select the leave mode for the specified downstream port(s) in this VLAN. This specifies whether the Switch removes an MLD snooping membership entry (learned on a downstream port) immediately (**Immediate**) or wait for an MLD report before the leave timeout (**Normal**) or fast leave timeout (**Fast**) when an MLD leave message is received on this port from a host.
Leave Timeout	Enter the MLD snooping normal leave timeout (in milliseconds) the Switch uses to update the forwarding table for the specified downstream port(s). This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.
Fast Leave Timeout	Enter the fast leave timeout (in milliseconds) for the specified downstream port(s). This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

23.4.4 MLD Snooping-proxy Filtering

Use this screen to configure the Switch's MLD filtering settings. Click the **MLD Snooping-proxy** link and then the **Filtering** link in the **Advanced Application > Multicast > IPv6 Multicast** screen to display the screen as shown. See Section 23.1 on page 227 for more information on multicasting.

Figure 164 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering (Standalone mode)

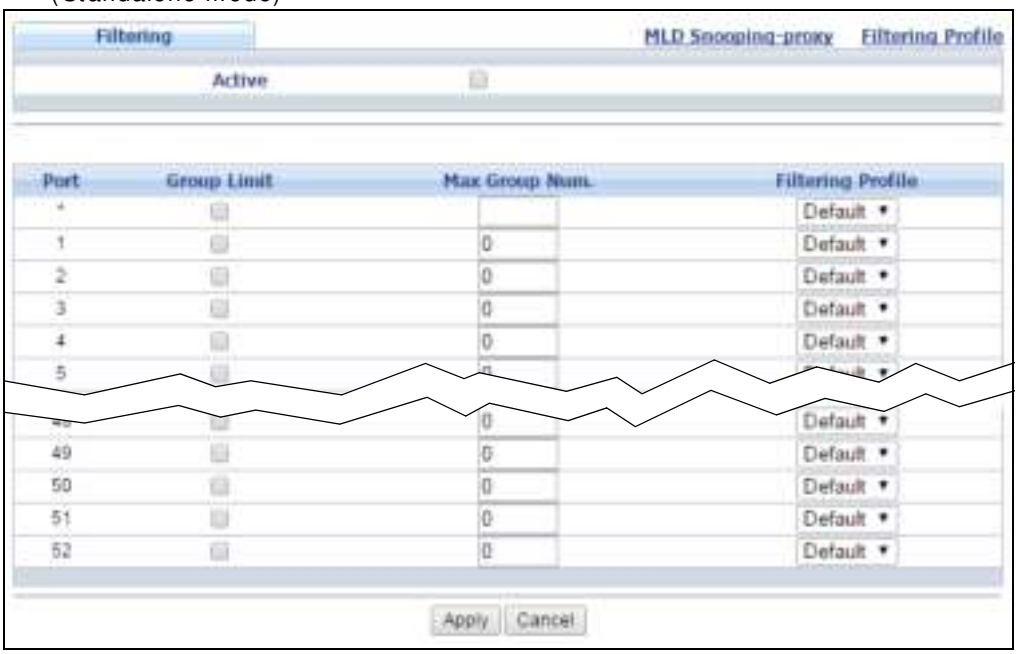
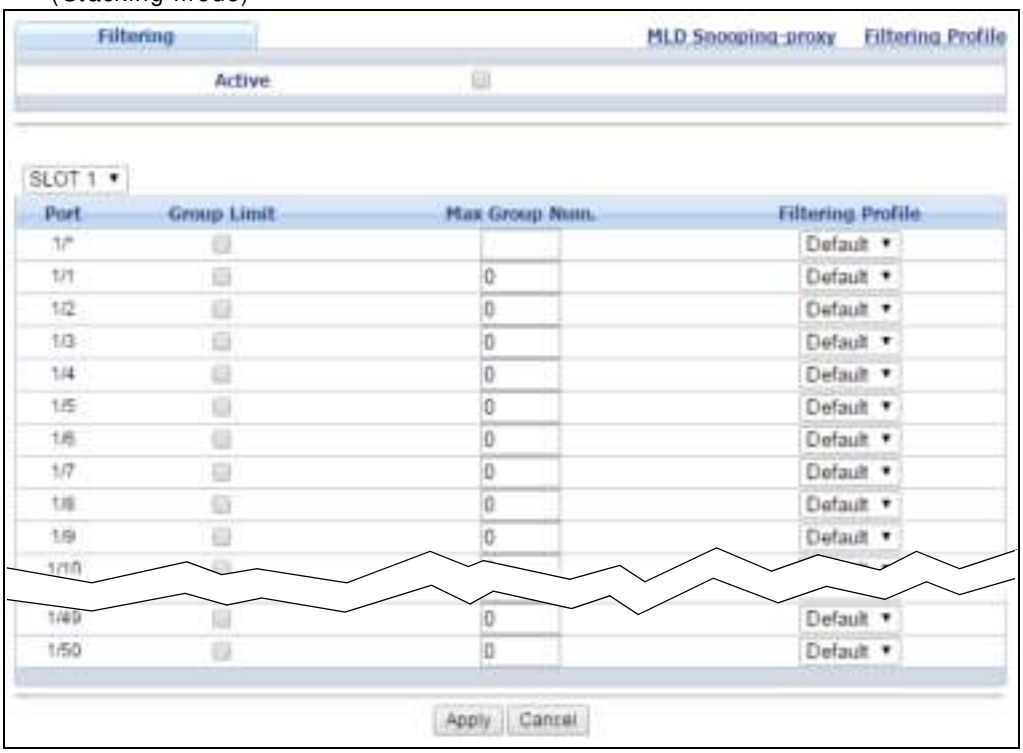


Figure 165 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering (Stacking mode)



The following table describes the labels in this screen.

Table 108 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering

LABEL	DESCRIPTION
Active	Select this option to enable MLD filtering on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Group Limit	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter 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 MLD Report message is dropped on this port.
Filtering Profile	Select the name of the MLD filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create MLD filtering profiles in the **Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile** screen.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

23.4.5 MLD Snooping-proxy Filtering Profile

Use this screen to create an MLD filtering profile and set the range of the multicast address(es). Click the **Filtering Profile** link in the **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering** screen to display the screen as shown.

Figure 166 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile

The following table describes the labels in this screen.

Table 109 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > 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 IPv6 address for a range of multicast IPv6 addresses that you want to belong to the MLD filtering profile.
End Address	Type the ending multicast IPv6 address for a range of IPv6 addresses that you want to belong to the MLD filtering profile. If you want to add a single multicast IPv6 address, enter it in both the **Start Address** and **End Address** fields.
Add	Click this to create a new entry. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to reset 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 IPv6 address range.
End Address	This field displays the end of the multicast IPv6 address range.
	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove, then click the **Delete** button. You can select the check box in the table heading row to select all profiles. To delete a rule(s) from a profile, select the rule(s) that you want to remove, then click the **Delete** button.
Delete	Click **Delete** button to permanently delete the entries you selected.
Cancel	Click **Cancel** to clear the check boxes.

23.5 MVR Overview

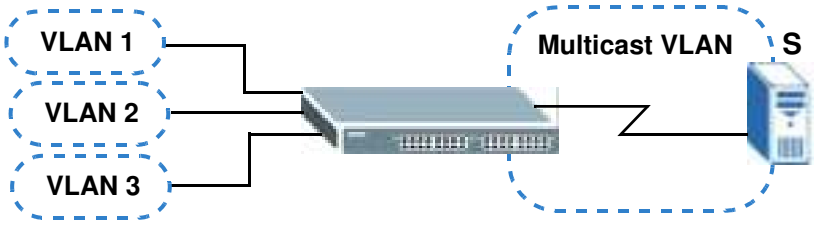
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

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 167 MVR Network Example



23.5.1 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.

23.5.2 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.

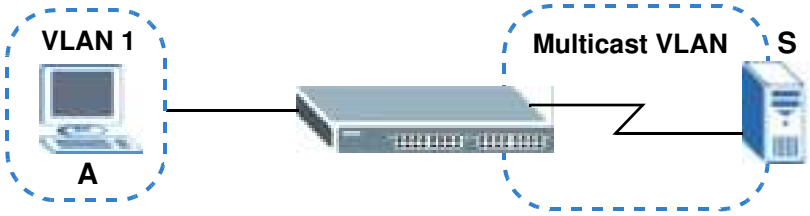
23.5.3 How MVR Works

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, an uplink 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 168 MVR Multicast Television Example



23.6 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 > MVR** to display the screen as shown next.

Note: You can create up to five 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 169 Advanced Application > Multicast > MVR (Standalone mode)

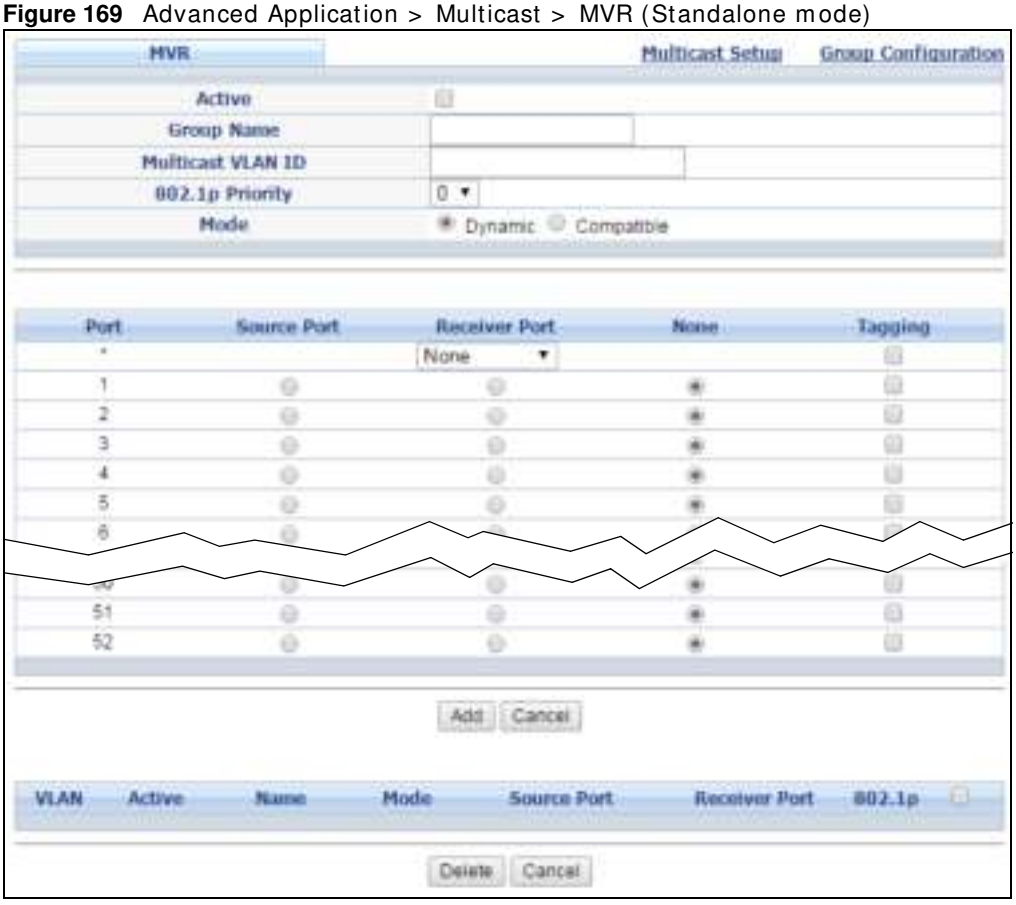
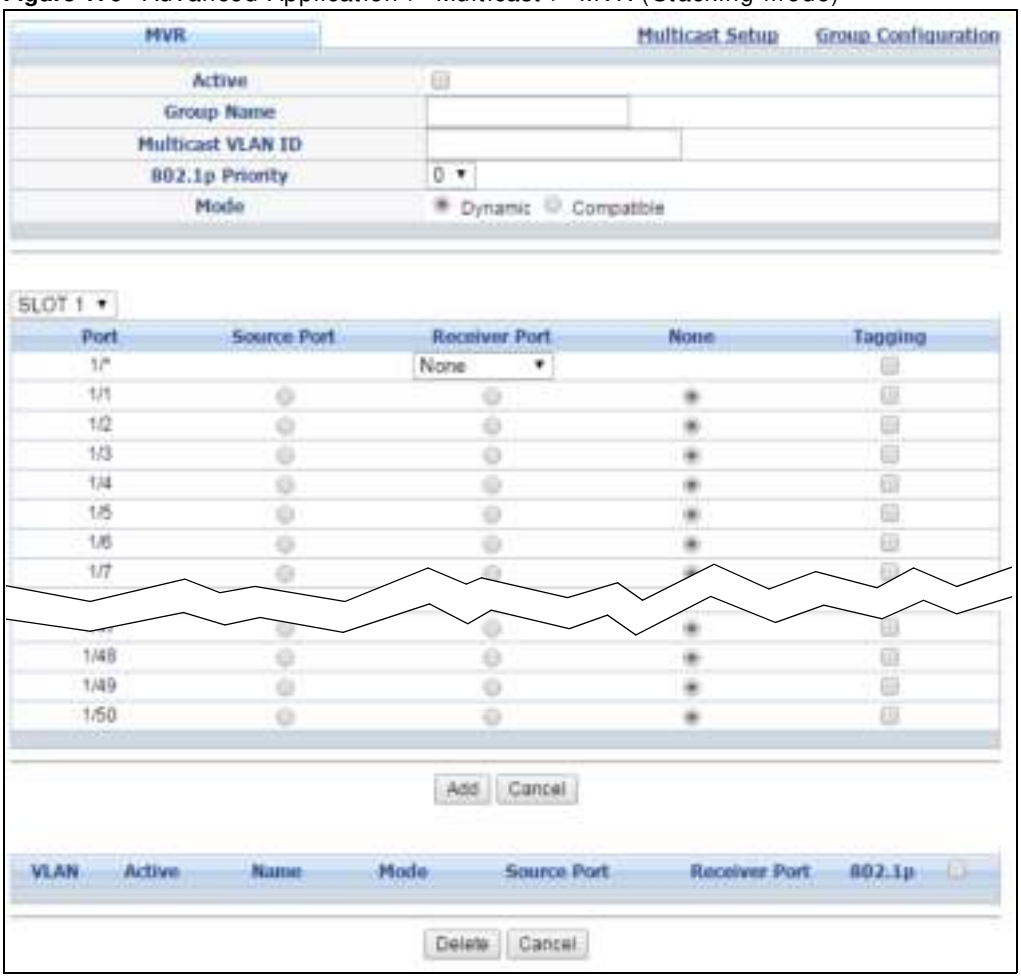


Figure 170 Advanced Application > Multicast > MVR (Stacking mode)



The following table describes the related labels in this screen.

Table 110 Advanced Application > Multicast > MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Group 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 or MLD control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports or MLD messages to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports or MLD messages.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 110 Advanced Application > Multicast > MVR (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. 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 this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID. Click on an index number to change the settings.
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.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove, then click the **Delete** button.
Cancel	Click **Cancel** to clear the check boxes.

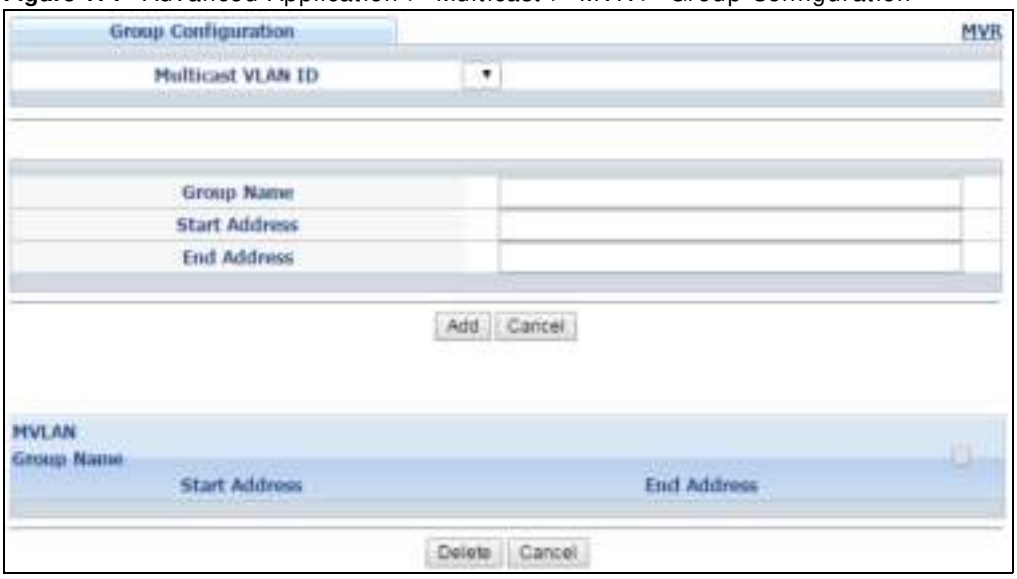
23.6.1 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Use this screen to configure MVR IP multicast group address(es). Click the **Group Configuration** link 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 171 Advanced Application > Multicast > MVR > Group Configuration



The following table describes the labels in this screen.

Table 111 Advanced Application > Multicast > MVR > Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Group Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 23.1.1 on page 227 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to Section 23.1.1 on page 227 for more information on IP multicast addresses.
Add	Click this to create a new entry. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Group 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	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove, then click the **Delete** button. You can select the check box in the table heading row to select all profiles. To delete a rule(s) from a profile, select the rule(s) that you want to remove, then click the **Delete** button.

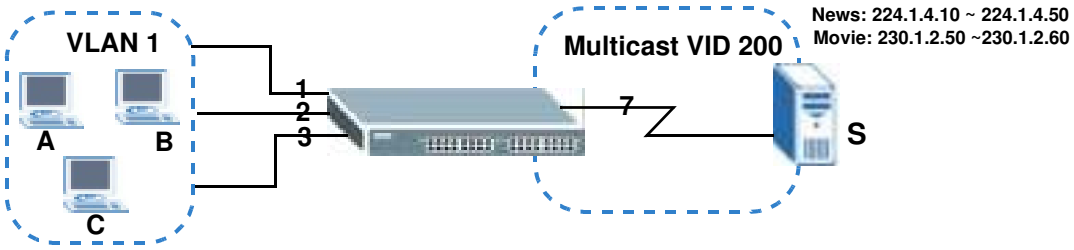
Table 111 Advanced Application > Multicast > MVR > Group Configuration (continued)

LABEL	DESCRIPTION
Delete	Select the entry(ies) that you want to remove, then click the **Delete** button to remove the selected entry(ies) from the table. If you delete a multicast VLAN, all multicast groups in this VLAN will also be removed.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

23.6.2 MVR Configuration Example

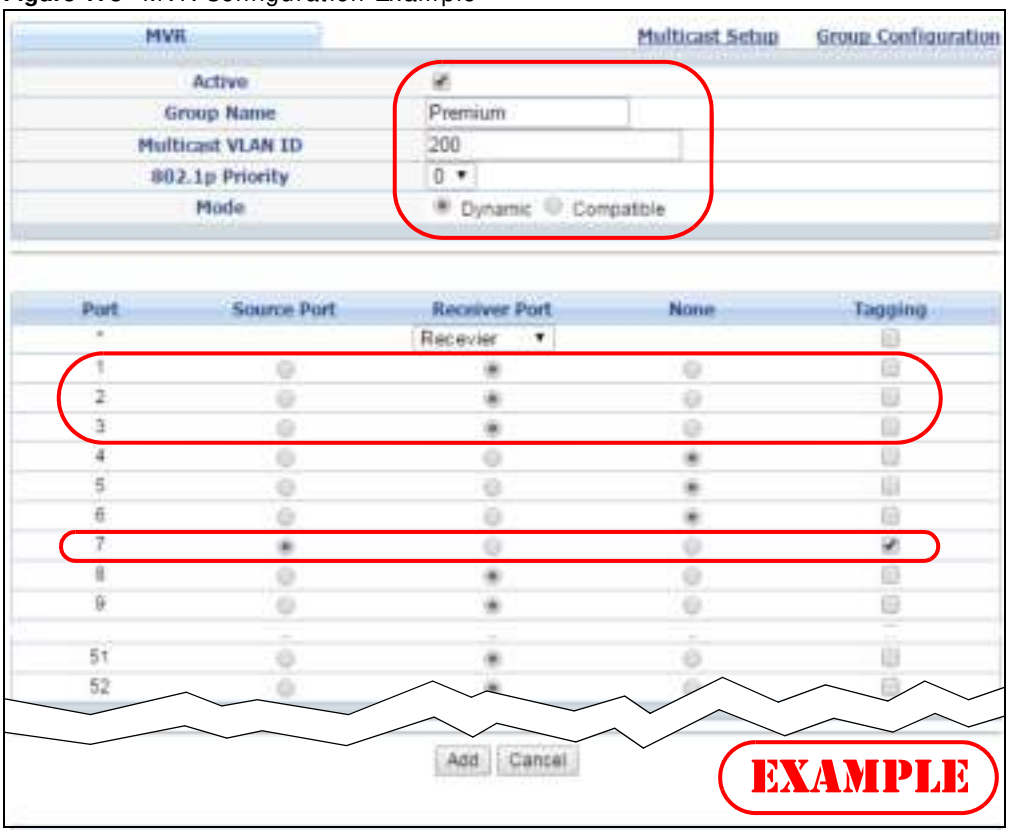
The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN 1 are able to receive the traffic.

Figure 172 MVR Configuration Example



To configure the MVR settings on the Switch, create a multicast VLAN in the **MVR** screen and set the receiver and source ports.

Figure 173 MVR Configuration Example



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 IPv4 multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 174 MVR Group Configuration Example

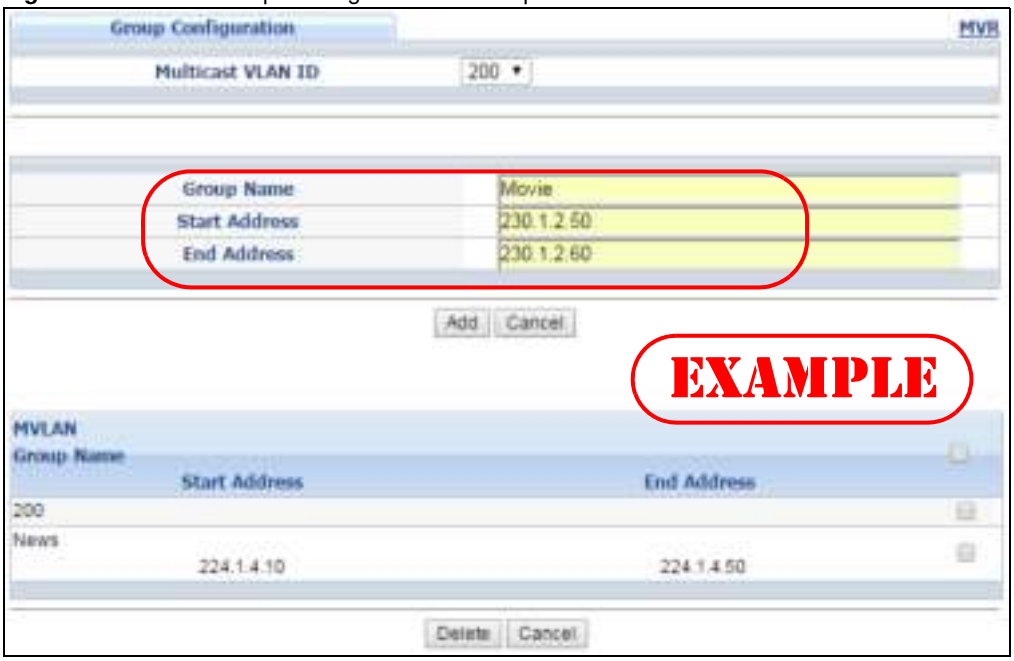
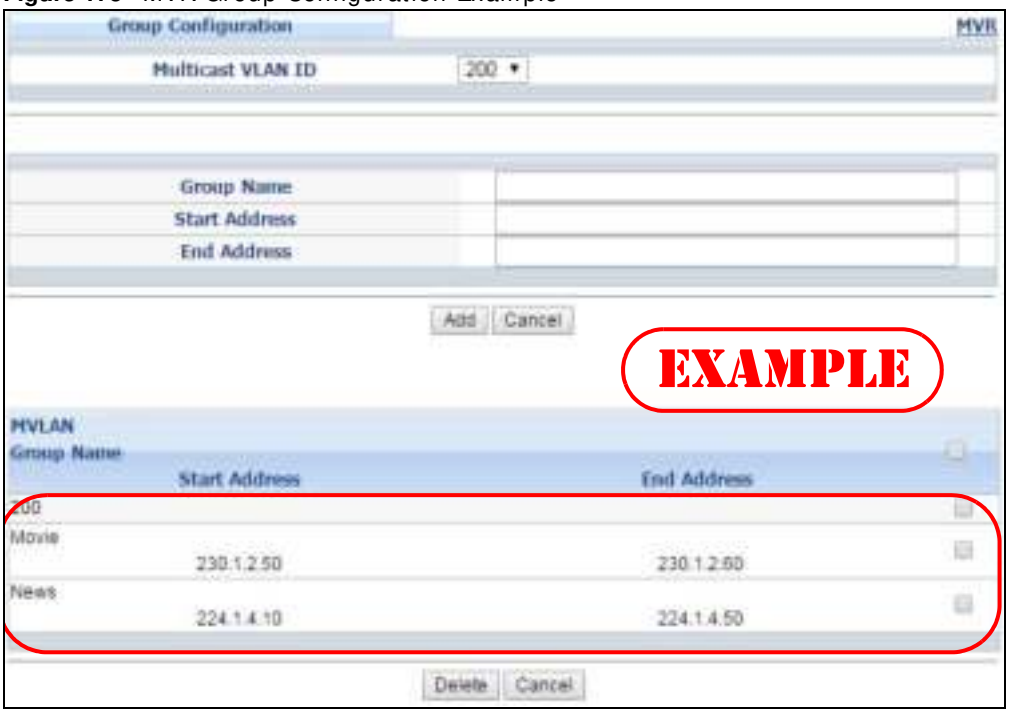


Figure 175 MVR Group Configuration Example



24

AAA

This chapter describes how to configure authentication, authorization and accounting settings on the Switch.

24.1 Authentication, Authorization and Accounting (AAA)

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 24.1.2 on page 254) and TACACS+ (Terminal Access Controller Access-Control System Plus, see Section 24.1.2 on page 254) as external authentication, authorization and accounting servers.

Figure 176 AAA Server

24.1.1 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 AAA server. However, there is a limit on the number of users you may authenticate in this way (See Chapter 48 on page 458).

24.1.2 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 112 RADIUS vs TACACS+

	RADIUS	TACACS+
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.

24.2 AAA Screens

The **AAA** screens allow you to enable authentication, authorization, accounting or all of them on the Switch. First, configure your authentication and accounting server settings (RADIUS, TACACS+ or both) and then set up the authentication priority, activate authorization and configure accounting settings.

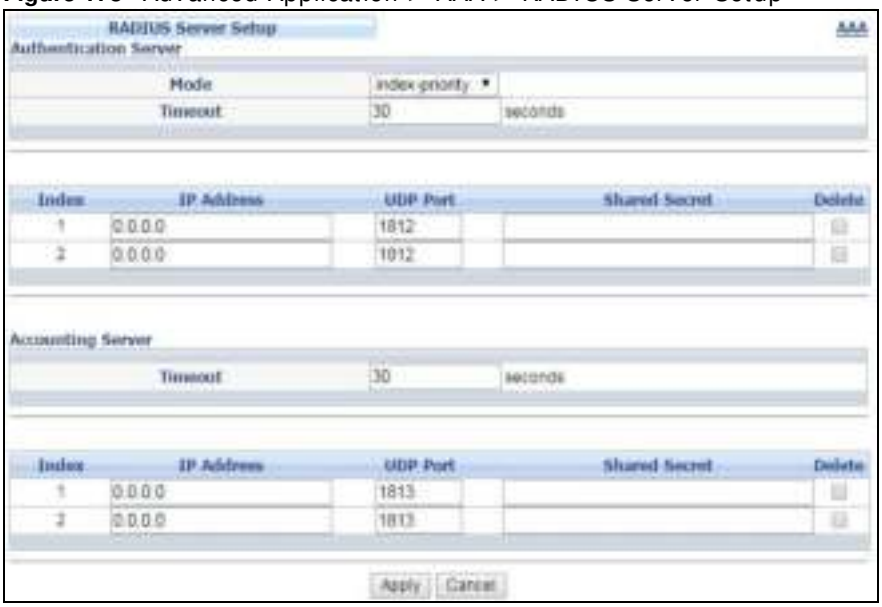
Click **Advanced Application** > **AAA** in the navigation panel to display the screen as shown.

Figure 177 Advanced Application > AAA

24.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See Section 24.1.2 on page 254 for more information on RADIUS servers and Section 24.3 on page 261 for RADIUS attributes utilized by the authentication and accounting features on the Switch. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 178 Advanced Application > AAA > RADIUS Server Setup



The following table describes the labels in this screen.

Table 113 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field only applies if you configure multiple RADIUS servers. Select **index-priority** 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 **round-robin** 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 **index-priority** 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 IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**. 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 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 **Apply**.
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.

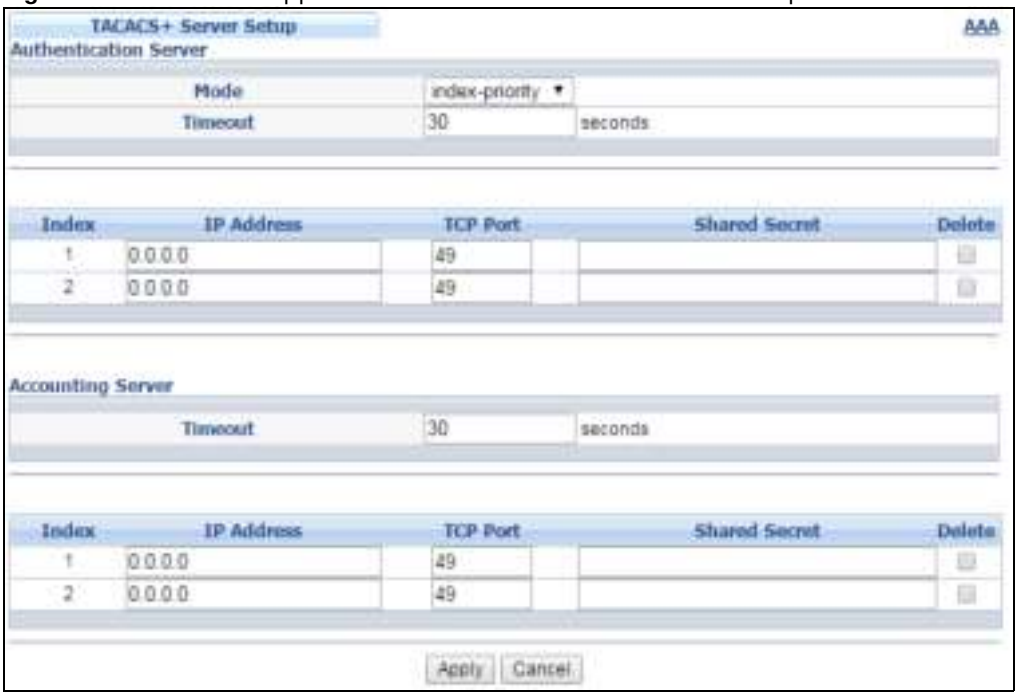
Table 113 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS accounting server for accounting is **1813**. 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 **Apply**.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See Section 24.1.2 on page 254 for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 179 Advanced Application > AAA > TACACS+ Server Setup



The following table describes the labels in this screen.

Table 114 Advanced Application > AAA > 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 **index-priority** 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 **round-robin** 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 **index-priority** 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 IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is **49**. 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+ 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 **Apply**.
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 IP address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ accounting server is **49**. 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 **Apply**.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.2.3 AAA Setup

Use this screen to configure authentication, authorization and accounting settings on the Switch. Click on the **AAA Setup** link in the **AAA** screen to view the screen as shown.

Figure 180 Advanced Application > AAA > AAA Setup

The following table describes the labels in this screen.

Table 115 Advanced Application > AAA > AAA Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Privilege Enable	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). Configure the access privilege of accounts via commands (see the Ethernet Switch CLI Reference Guide) for **local** authentication. The **TACACS+** and **RADIUS** are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. 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 **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for access privilege level specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the access privilege configured for local authentication. Select **radius** or **tacacs+** to have the Switch check the access privilege via the external servers.

Table 115 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the **Access Control > Logins** screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. 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 **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for administrator accounts, specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the administrator accounts configured in the **Access Control > Logins** screen. Select **radius** to have the Switch check the administrator accounts configured via the RADIUS Server. Select **tacacs+** to have the Switch check the administrator accounts configured via the TACACS+ Server**.**
Authorization	Use this section to configure authorization settings on the Switch.
Type	Set whether the Switch provides the following services to a user. • **Exec**: Allow an administrator which logs in the Switch through Telnet or SSH to have different access privilege level assigned via the external server. • **Dot1x**: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.
Console	Select this to allow an administrator which logs in the Switch through the console port to have different access privilege level assigned via the external server.
Method	Select whether you want to use RADIUS or TACACS+ for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
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 **start-stop** option for the **Exec** or **Dot1x** entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • **System** - 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 • **Exec** - Configure the Switch to send information when an administrator logs in and logs out via the console port, telnet or SSH. • **Dot1x** - 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. • **Commands** - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. 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.

Table 115 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Mode	The Switch supports two modes of recording login events. Select: • **start-stop** - 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 **Update Period**), and when a user ends a session. • **stop-only** - to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events. TACACS+ is the only method for recording **Commands** type of event.
Privilege	This field is only configurable for **Commands** 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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.2.4 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. Note that these attributes only work when you enable authorization (see Section 24.2.3 on page 257).

Table 116 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **1** Vendor-data = ingress rate (Kbps in decimal format)
Egress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **2** Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = **890** Vendor-Type = **3** Vendor-Data = "**shell:priv-lvl=**N" or Vendor-ID = **9** (CISCO) Vendor-Type = **1** (CISCO-AVPAIR) Vendor-Data = "**shell:priv-lvl=**N" 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.

24.2.5 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 these attributes only work when you enable authorization (see Section 24.2.3 on page 257).

Table 117 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = **VLAN(13)** Tunnel-Medium-Type = **802(6)** Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch. Note: The bolded values in this table are fixed values as defined in RFC 3580.

24.3 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 RADIUS attributes used for accounting.

This section lists the attributes used by authentication and accounting functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

24.3.1 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

24.3.1.1 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

24.3.1.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

24.3.1.3 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

24.3.2 Attributes Used for Accounting

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

24.3.2.1 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, 200704191721030000000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

24.3.2.2 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 118 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-IP-Address	✔	✔	✔
Service-Type	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Session-Time		✔	✔
Acct-Terminate-Cause			✔

Table 119 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-IP-Address	✔	✔	✔
Service-Type	✔	✔	✔
Calling-Station-Id	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Session-Time		✔	✔
Acct-Terminate-Cause			✔

24.3.2.3 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 120 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-IP-Address	✔	✔	✔
NAS-Port	✔	✔	✔
Class	✔	✔	✔
Called-Station-Id	✔	✔	✔
Calling-Station-Id	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-Port-Type	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Input-Octets		✔	✔
Acct-Output-Octets		✔	✔
Acct-Session-Time		✔	✔
Acct-Input-Packets		✔	✔
Acct-Output-Packets		✔	✔
Acct-Terminate-Cause			✔
Acct-Input-Gigawords		✔	✔
Acct-Output-Gigawords		✔	✔

25

IP Source Guard

25.1 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.

25.1.1 What You Can Do

- Use the **IP Source Guard** screen (Section 25.2 on page 267) to look at the current bindings for DHCP snooping and ARP inspection.
- Use the **IP Source Guard Static Binding** screen (Section 25.4 on page 269) to manage static bindings for DHCP snooping and ARP inspection.
- Use the **DHCP Snooping** screen (Section 25.5 on page 271) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Configure** screen (Section 25.6 on page 273) 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.
- Use the **DHCP Snooping Port Configure** screen (Section 25.6.1 on page 275) to specify whether ports are trusted or untrusted ports for DHCP snooping.

- Use the **DHCP Snooping VLAN Configure** screen (Section 25.6.2 on page 277) to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.
- Use the **DHCP Snooping VLAN Port Configure** screen (Section 25.6.3 on page 278) to apply a different DHCP option 82 profile to certain ports in a VLAN.
- Use the **ARP Inspection Status** screen (Section 25.7 on page 279) to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet.
- Use the **ARP Inspection VLAN Status** screen (Section 25.7.1 on page 280) to look at various statistics about ARP packets in each VLAN.
- Use the **ARP Inspection Log Status** screen (Section 25.7.2 on page 281) to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
- Use the **ARP Inspection Configure** screen (Section 25.8 on page 282) 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.
- Use the **ARP Inspection Port Configure** screen (Section 25.8.1 on page 284) to specify whether ports are trusted or untrusted ports for ARP inspection.
- Use the **ARP Inspection VLAN Configure** screen (Section 25.8.2 on page 286) to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN.
- Use the **Advanced Application > IP Source Guard > IPv6 Source Binding Status** screen (Section 25.10 on page 287) to look at the current IPv6 dynamic and static bindings and to remove dynamic bindings based on IPv6 address and/or IPv6 prefix.
- Use the **Advanced Application > IP Source Guard > IPv6 Static Binding Setup** screen (Section 25.11 on page 288) to manually create an IPv6 source guard binding table and manage IPv6 static bindings.
- Use the **Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup** screen (Section 25.12 on page 290) to have IPv6 source guard forward valid IPv6 addresses and/or IPv6 prefixes that are stored in the binding table and allow or block data traffic from all link-local addresses.
- Use the **Advanced Application > IP Source Guard > IPv6 Source Guard Port Setup** screen (Section 25.13 on page 291) to apply configured IPv6 source guard policies to the ports you specify.
- Use the **Advanced Application > IP Source Guard > IPv6 Snooping Policy Setup** screen (Section 25.14 on page 292) to dynamically create an IPv6 source guard binding table using a DHCPv6 snooping policy. A DHCPv6 snooping policy lets the Switch sniff DHCPv6 packets sent from a DHCPv6 server to a DHCPv6 client when it is assigning an IPv6 address.
- Use the **Advanced Application > IP Source Guard > IPv6 Snooping VLAN Setup** screen (Section 25.15 on page 293) to enable a DHCPv6 snooping policy on a specific VLAN interface.
- Use the **Advanced Application > IP Source Guard > IPv6 DHCP Trust Setup** screen (Section 25.16 on page 294) to specify which ports are trusted and untrusted for DHCP snooping.

25.1.2 What You Need to Know

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.

25.2 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 181 IP Source Guard (Standalone mode)

Figure 182 IP Source Guard (Stacking mode)

The following table describes the labels in this screen.

Table 121 IP Source Guard

LABEL	DESCRIPTION
IPv4 Source Guard Setup	Click the link to open screens where you can view and manage static bindings, configure DHCP snooping or ARP inspection and look at various statistics.
IPv6 Source Binding Status (Standalone mode)	Click the link to open a screen where you can view the current IPv6 dynamic and static bindings or remove dynamic bindings based on IPv6 address and/or IPv6 prefix.
IPv6 Static Binding Setup (Standalone mode)	Click the link to open a screen where you can manually create IPv6 source guard static binding entries.
IPv6 Source Guard Policy Setup (Standalone mode)	Click the link to open a screen where you can define policies to have IPv6 source guard forward valid addresses and/or prefixes and allow or block data traffic from all link-local addresses.

Table 121 IP Source Guard (continued)

LABEL	DESCRIPTION
IPv6 Source Guard Port Setup (Standalone mode)	Click the link to open a screen where you can apply the configured IPv6 source guard policy to a port.
IPv6 Snooping Policy Setup (Standalone mode)	Click the link to open a screen where you can set up DHCPv6 snooping policies for the binding table.
IPv6 Snooping VLAN Setup (Standalone mode)	Click the link to open a screen where you can enable a DHCPv6 snooping policy on a specific VLAN interface.
IPv6 DHCP Trust Setup (Standalone mode)	Click the link to open a screen where you can specify which ports are trusted for DHCPv6 snooping.

25.3 IPv4 Source Guard Setup

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 > IPv4 Source Guard Setup**.

Figure 183 Advanced Application > IP Source Guard > IPv4 Source Guard Setup

The following table describes the labels in this screen.

Table 122 Advanced Application > IP Source Guard > IPv4 Source Guard Setup

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, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator. **dhcp-snooping**: 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.

25.4 IPv4 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 > IPv4 Source Guard Setup > Static Binding**.

Figure 184 IP Source Guard > IPv4 Source Guard Setup > Static Binding (Standalone mode)

Figure 185 IP Source Guard > IPv4 Source Guard Setup > Static Binding (Stacking mode)

The following table describes the labels in this screen.

Table 123 IP Source Guard > IPv4 Source Guard Setup > Static Binding

LABEL	DESCRIPTION
ARP Freeze	ARP Freeze allows you to automatically create static bindings from the current ARP entries (either dynamically learned or static ARP entries) until the Switch's binding table is full. Note: The ARP learning mode should be set to **ARP-Request** in the **IP Application > ARP Setup > ARP Learning** screen before you use the ARP Freeze feature.
Condition	**All** - Select this and click **ARP Freeze** to have the Switch automatically add all the current ARP entries to the static bindings table. **Port List** - Select this and enter the number of the port(s) (separated by a comma). In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example. ARP entries learned on the specified port(s) are added to the static bindings table after you click **ARP Freeze**. **VLAN List** - Select this and enter the ID number of the VLAN(s) (separated by a comma). ARP entries for the specified VLAN(s) are added to the static bindings table after you click **ARP Freeze**.
Static Binding	
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. In stacking mode, the first field is the slot ID and the second field is the port number. If this binding applies to all ports, select **Any**.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** 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 above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each binding. Click on an index number to view more details or change the settings.
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. **static**: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 123 IP Source Guard > IPv4 Source Guard Setup > Static Binding (continued)

LABEL	DESCRIPTION
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the entry(ies) that you want to remove, then click the **Delete** button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the check boxes above.

25.5 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 > IPv4 Source Guard Setup > DHCP Snooping**.

Figure 186 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping

The following table describes the labels in this screen.

Table 124 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping

LABEL	DESCRIPTION
Database Status	
	This section displays the current settings for the DHCP snooping database. You can configure them in the **DHCP Snooping Configure** screen. See Section 25.6 on page 273.
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. **none**: The Switch is not accessing the DHCP snooping database. **read**: The Switch is loading dynamic bindings from the DHCP snooping database. **write**: 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 **Not Running** 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 **Not Running** 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 124 IP Source Guard > IPv4 Source Guard Setup > 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 Ethernet Switch 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 Ethernet Switch 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.

25.6 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 > IPv4 Source Guard Setup > DHCP Snooping > Configure**.

Figure 187 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure

The following table describes the labels in this screen.

Table 125 IP Source Guard > IPv4 Source Guard Setup > 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: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
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 select an option 82 profile in the **DHCP Snooping VLAN Configure** screen (Section 25.6.2 on page 277) to help the DHCP servers distinguish between DHCP requests from different VLAN. Select **Disable** if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database	If **Timeout interval** is greater than **Write delay interval**, 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: **tftp:**/ / **{ domain name or IP address}** / **directory, if applicable**/ **file name**; for example, **tftp:**/ / **192.168.10.1**/ **database.txt.**
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.
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.

Table 125 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure (continued)

LABEL	DESCRIPTION
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click **Renew** 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 **Agent URL**. 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 **Binding collisions** counter in the **DHCP Snooping** screen (Section 25.5 on page 271).
Apply	Click **Apply** 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 **Save** 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.

25.6.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

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 > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**.

Figure 188 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure> Port (Standalone mode)_

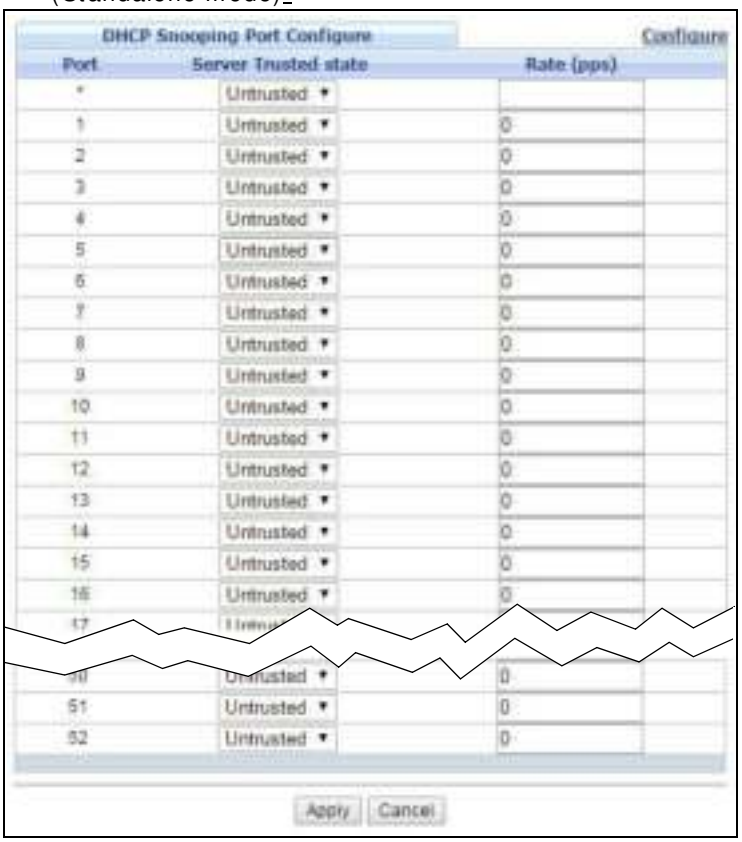
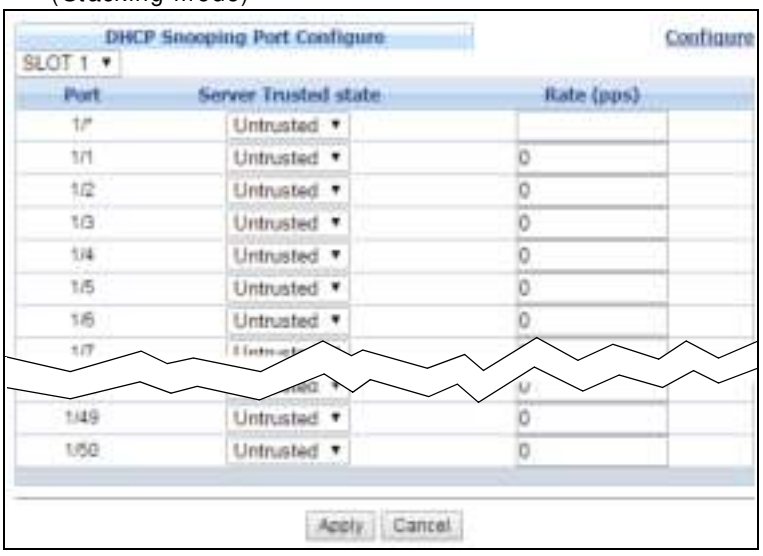


Figure 189 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure> Port (Stacking mode)



The following table describes the labels in this screen.

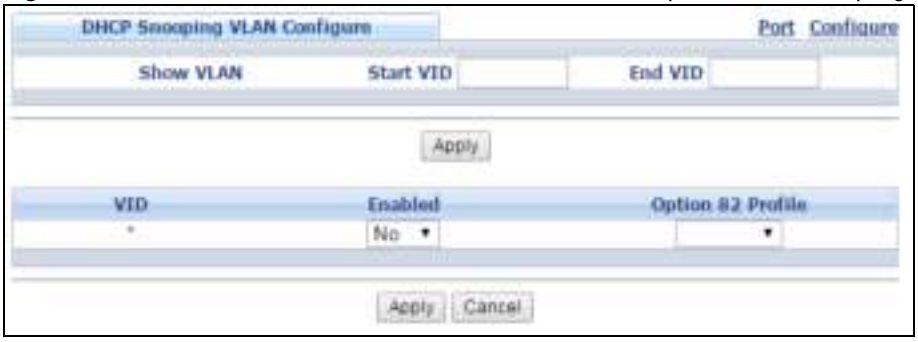
Table 126 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
Server Trusted state	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). 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 **Apply** 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 **Save** 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.

25.6.2 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 43 on page 413) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN**.

Figure 190 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN



The following table describes the labels in this screen.

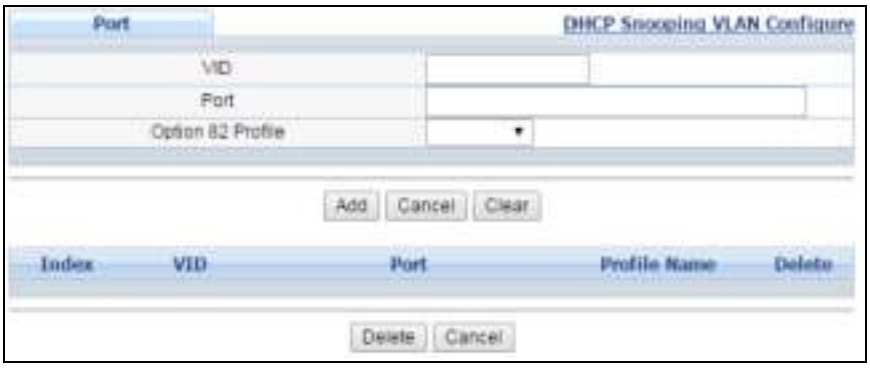
Table 127 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN

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 **Yes** to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in the specified VLAN(s). The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen (see Section 25.6 on page 273).
Apply	Click **Apply** 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 **Save** 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.

25.6.3 DHCP Snooping VLAN Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. To open this screen, click **Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN > Port**.

Figure 191 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN > Port



The following table describes the labels in this screen.

Table 128 IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN > Port

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s) in this VLAN. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen (see Section 25.6 on page 273). Note: The profile you select here has priority over the one you select in the **DHCP Snooping > Configure > VLAN** screen.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** 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 above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the port(s) belongs.
Port	This field displays the port(s) to which the Switch applies the settings. In stacking mode, the first number represents the slot and the second the port number.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s).
Delete	Select the entry(ies) that you want to remove in the **Delete** column, then click the **Delete** button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the **Delete** check boxes above.

25.7 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 > IPv4 Source Guard Setup > ARP Inspection**.

Figure 192 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection Status

The following table describes the labels in this screen.

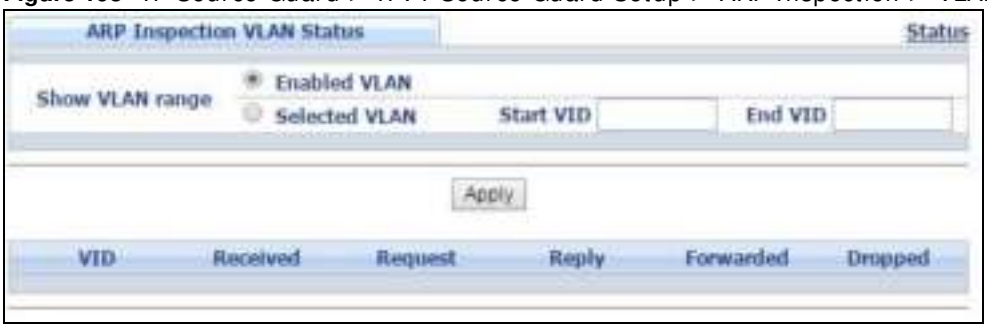
Table 129 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection Status

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. In stacking mode, the first field is the slot ID and the second field is the port number.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).
Reason	This field displays the reason the ARP packet was discarded. **MAC+ VLAN**: The MAC address and VLAN ID were not in the binding table. **IP**: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. **Port**: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the **Delete** check boxes above.
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

25.7.1 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 > IPv4 Source Guard Setup > ARP Inspection > VLAN Status**.

Figure 193 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > VLAN Status



The following table describes the labels in this screen.

Table 130 IP Source Guard > IPv4 Source Guard Setup > 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 (**Start VID**) and the highest VLAN ID (**End VID**) 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.

25.7.2 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 > IPv4 Source Guard Setup > ARP Inspection > Log Status**.

Figure 194 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Log Status

The following table describes the labels in this screen.

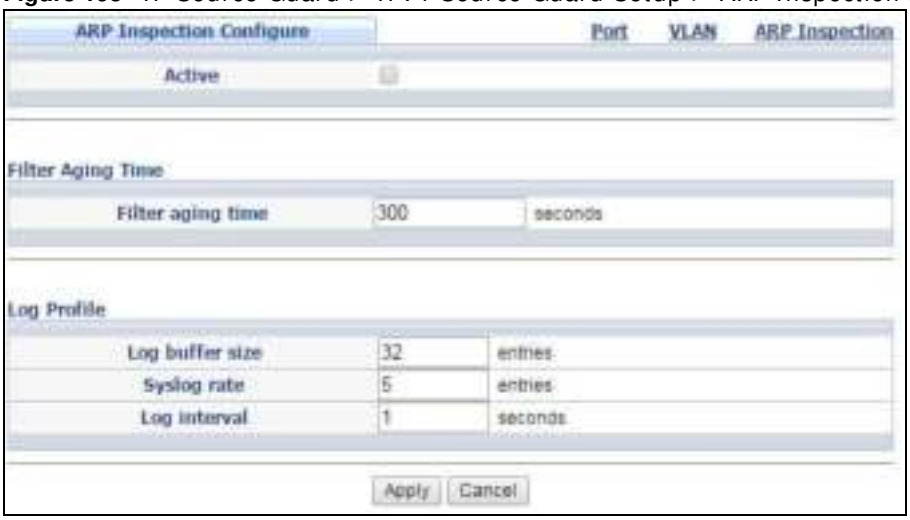
Table 131 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Log Status

LABEL	DESCRIPTION
Clearing log status table	Click **Apply** 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 **overflow** 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. In stacking mode, the first field is the slot ID and the second field is the port number.
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 **ARP Inspection Configure** screen. See Section 25.8 on page 282.
Reason	This field displays the reason the log message was generated. **dhcp deny**: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **dhcp permit**: An ARP packet was forwarded because it matched a dynamic binding. **static permit**: An ARP packet was forwarded because it matched a static binding. In the **ARP Inspection VLAN Configure** 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 Section 25.8.2 on page 286.
Time	This field displays when the log message was generated.

25.8 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 > IPv4 Source Guard Setup > ARP Inspection > Configure**.

Figure 195 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure



The following table describes the labels in this screen.

Table 132 IP Source Guard > IPv4 Source Guard Setup > 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. Type 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 **Syslog rate** and **Log interval**. 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 **Clearing log status table** in the **ARP Inspection Log Status** screen to clear the log and reset this counter. See Section 25.7.2 on page 281.
Syslog rate	Type 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 **Log Interval**. You must configure the syslog server (Chapter 50 on page 485) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between **Syslog rate** and **Log interval** is illustrated in the following examples: • 4 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 1: the Switch sends 4 syslog messages every second. • 6 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 2: the Switch sends 5 syslog messages every 2 seconds.
Log interval	Type 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 **Syslog rate** for an example of the relationship between **Syslog rate** and **Log interval**.

Table 132 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** 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.

25.8.1 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 > IPv4 Source Guard Setup > ARP Inspection > Configure > Port**.

Figure 196 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port (Standalone mode)

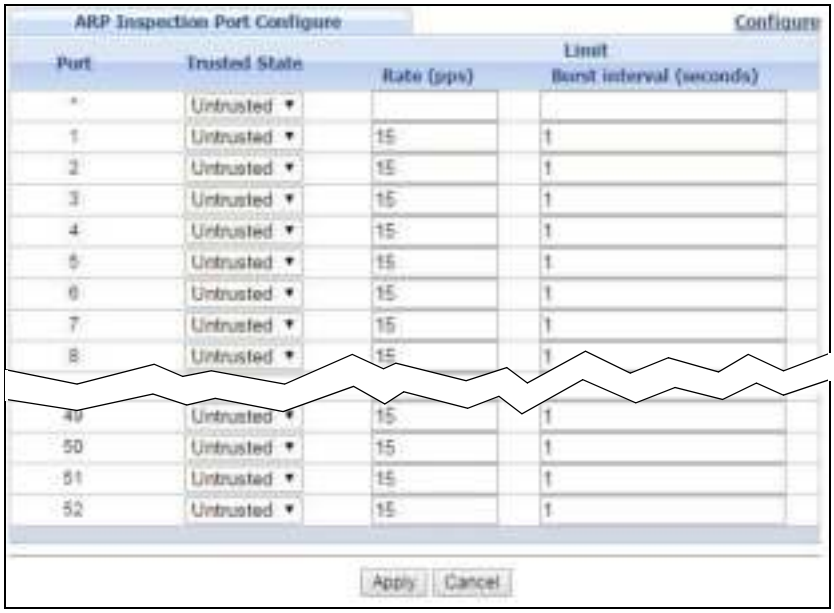
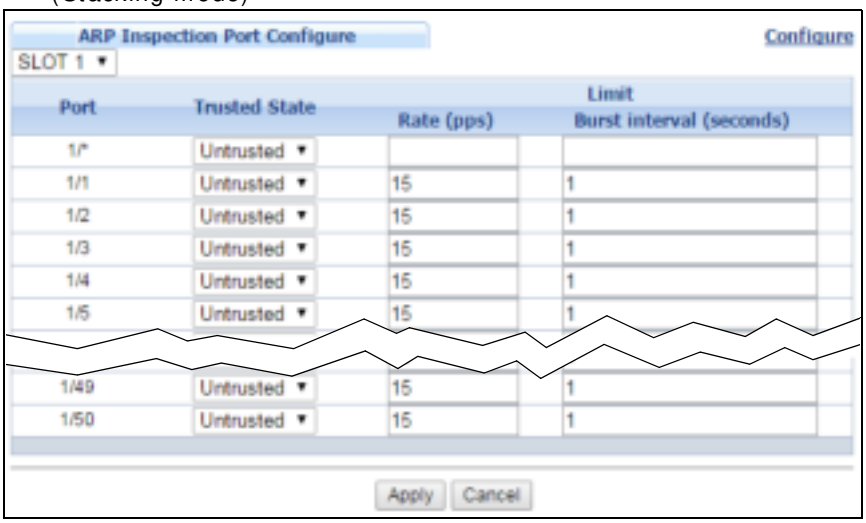


Figure 197 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port (Stacking mode)



The following table describes the labels in this screen.

Table 133 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). 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	Rate and Burst Interval 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.
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 **Apply** 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 **Save** 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.

25.8.2 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 > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN**.

Figure 198 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN

The following table describes the labels in this screen.

Table 134 IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN

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 **Yes** to enable ARP inspection on the VLAN. Select **No** to disable ARP inspection on the VLAN.
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. **None**: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. **Deny**: The Switch generates log messages when it discards an ARP packet from the VLAN. **Permit**: The Switch generates log messages when it forwards an ARP packet from the VLAN. **All**: The Switch generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click **Apply** 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 **Save** 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.

25.9 IPv6 Source Guard Overview

The purpose of IPv6 source guard is to distinguish between authorized and unauthorized users by using a binding table that validates the source of IPv6 traffic. The binding table can be manually created or be learned through Dynamic Host Configuration Protocol version 6 snooping (DHCPv6 snooping). IPv6 source guard can deny IPv6 traffic from an unknown source. The IPv6 source guard binding table includes:

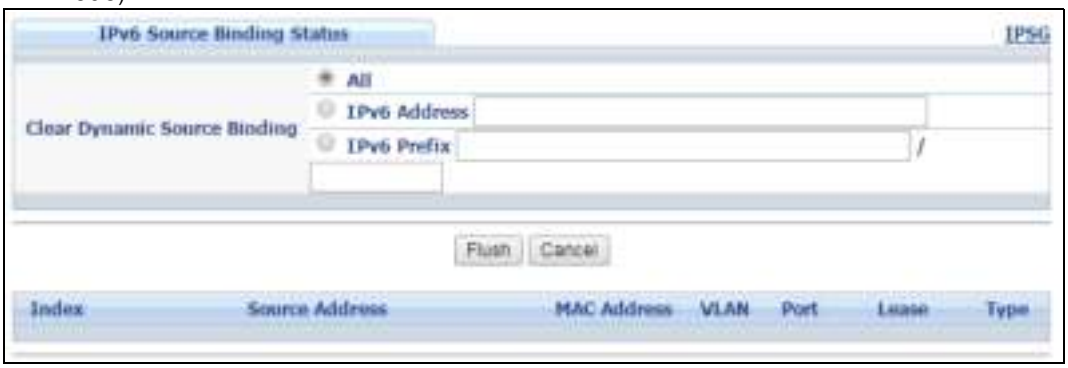
- IPv6 address
- IPv6 prefix
- VLAN ID
- Port number
- MAC address

Enable IPv6 source guard on a port for the Switch to check incoming IPv6 packets on that port. A packet is allowed when it matches any entry in the IPSG binding table. If a user tries to send IPv6 packets to the Switch that do not match an entry in the IPSG binding table, the Switch will drop these packets. The Switch forwards matching traffic normally. The IPv6 source guard related screens are available in standalone mode.

25.10 IPv6 Source Binding Status

Use this screen to look at the current IPv6 dynamic and static bindings and to remove dynamic bindings based on IPv6 address and/or IPv6 prefix. Bindings are used 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 > IPv6 Source Binding Status**.

Figure 199 Advanced Application > IP Source Guard > IPv6 Source Binding Status (Standalone mode)



The following table describes the labels in this screen.

Table 135 Advanced Application > IP Source Guard > IPv6 Source Binding Status (Standalone mode)

LABEL	DESCRIPTION
Clear Dynamic Source Binding	Specify how you want the Switch to remove dynamic IPv6 source binding entries when you click **Flush**. • Select **All** to remove all of the dynamic entries from the IPv6 source binding table. • Select **IPv6 Address** and enter an IPv6 address to remove the dynamic entries snooped with the specified IPv6 address. • Select **IPv6 Prefix** and enter a Prefix address to remove the dynamic entries snooped with the specified Prefix address.
Flush	Click this to remove dynamic IPv6 source binding entries according to your selections.
Cancel	Click this to reset the values above based or if not applicable, to clear the fields above.
Index	This field displays a sequential number for each binding.
Source Address	This field displays the source IP address in the binding. If the entry is blank, this field will not be checked in the binding.
MAC Address	This field displays the source MAC address in the binding. If the entry is blank, this field will not be checked in the binding.
VLAN	This field displays the source VLAN ID in the binding. If the entry is blank, this field will not be checked in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. **S**: This static binding was learned from information provided manually by an administrator. **DH**: This dhcp-snooping binding was learned by snooping DHCP packets.

25.11 IPv6 Static Binding Setup

Use this screen to manually create an IPv6 source guard binding table entry and manage IPv6 static bindings. Static bindings are uniquely identified by the source IPv6 address / prefix. Each source IPv6 address / prefix can only be in one static binding. If you try to create a static binding with the same source IPv6 address / prefix as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > IPv6 Static Binding Setup**.

Figure 200 Advanced Application > IP Source Guard > IPv6 Static Binding Setup (Standalone mode)

The following table describes the labels in this screen.

Table 136 Advanced Application > IP Source Guard > IPv6 Static Binding Setup (Standalone mode)

LABEL	DESCRIPTION
IPv6 Static Binding	
Source Address	Enter the IPv6 address or IPv6 prefix and prefix length in the binding.
MAC Address	Enter the source MAC address in the binding. If this binding doesn't check this field, select **Any**. Note: You cannot choose **Any** for all three of **MAC Address**, **VLAN** and **Port**. You must fill in at least one.
VLAN	Enter the source VLAN ID in the binding. If this binding doesn't check this field, select **Any**.
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 **Any**.
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based 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.
Source Address	This field displays the IPv6 address or IPv6 prefix and prefix length in the binding.
MAC Address	This field displays the source MAC address in the binding. If the entry is blank, this field will not be checked in the binding.
VLAN	This field displays the source VLAN ID in the binding. If the entry is blank, this field will not be checked 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 an entry checkbox and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

25.12 IPv6 Source Guard Policy Setup

Use this screen to have IPv6 source guard forward valid IPv6 addresses and/or IPv6 prefixes that are stored in the binding table and allow or block data traffic from all link-local addresses. To open this screen, click **Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup**.

- If you select **Validate Address** and not **Validate Prefix**, traffic for a binding entry that matches a IPv6 address and VLAN ID, port number, and MAC address will be forwarded. If this binding entry is a IPv6 prefix, the traffic will be denied.
- If you select **Validate Prefix** and not **Validate Address**, traffic for a binding entry that matches a IPv6 prefix and VLAN ID, port number, and MAC address will be forwarded. If this binding entry is a IPv6 address, the traffic will be denied.
- If you select both **Validate Prefix** and **Validate Address** then traffic matching either IPv6 address or prefix will be forwarded.

Figure 201 Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup (Standalone mode)

The following table describes the labels in this screen.

Table 137 Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup (Standalone mode)

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes for this IPv6 source guard policy.
Validate Address	Select **Validate Address** to have IPv6 source guard forward valid addresses that are stored in the binding table.
Validate Prefix	Select **Validate Prefix** to have IPv6 source guard forward valid prefixes that are stored in the binding table.
Link Local	Select **Permit** to allow data traffic from all link-local addresses; otherwise leave the setting at **Deny**. A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format.
Add	Click this to create the IPv6 source guard policy or to update an existing one.
Cancel	Click this to reset the values above 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 policy.
Name	This field displays the descriptive name for identification purposes for this IPv6 source guard policy.
Validate Address	This field displays the **Validate Address** status for this IPv6 source guard policy.

Table 137 Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup (Standalone mode)

LABEL	DESCRIPTION
Validate Prefix	This field displays the **Validate Prefix** status for this IPv6 source guard policy.
Link Local	This field displays the **Link Local** traffic status for this IPv6 source guard policy.
Delete	Select an entry checkbox and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

25.13 IPv6 Source Guard Port Setup

Use this screen to apply configured IPv6 source guard policies to ports you specify. Use port * to apply a policy to all ports. To open this screen, click **Advanced Application > IP Source Guard > IPv6 Source Guard Port Setup**.

Figure 202 Advanced Application > IP Source Guard > IPv6 Source Guard Port Setup (Standalone mode)

The following table describes the labels in this screen.

Table 138 Advanced Application > IP Source Guard > IPv6 Source Guard Port Setup (Standalone mode)

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Policy Name	Select an IPv6 source guard policy that the Switch will apply to this port.

Table 138 Advanced Application > IP Source Guard > IPv6 Source Guard Port Setup (Standalone mode)

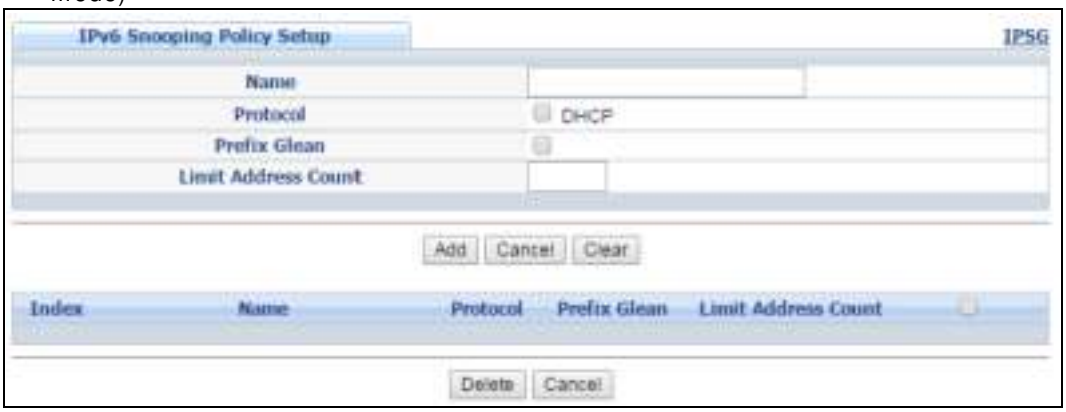
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.14 IPv6 Snooping Policy Setup

Use this screen to dynamically create an IPv6 source guard binding table using a DHCPv6 snooping policy. A DHCPv6 snooping policy lets the Switch sniff DHCPv6 packets sent from a DHCPv6 server to a DHCPv6 client when it is assigning an IPv6 address. When a DHCPv6 client successfully gets a valid IPv6 address, DHCPv6 snooping builds the binding table dynamically. To open this screen, click **Advanced Application > IP Source Guard > IPv6 Snooping Policy Setup**.

Note: If you do not select **Protocol** and **Prefix Glean**, then the Switch cannot perform DHCPv6 snooping.

Figure 203 Advanced Application > IP Source Guard > IPv6 Snooping Policy Setup (Standalone mode)



The following table describes the labels in this screen.

Table 139 Advanced Application > IP Source Guard > IPv6 Snooping Policy Setup (Standalone mode)

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes for this IPv6 snooping policy.
Protocol	Select **DHCP** to let the Switch sniff DHCPv6 packets sent from a DHCPv6 server to a DHCPv6 client.
Prefix Glean	Select this to learn the IPv6 prefix and length from DHCPv6 sniffed packets.
Limit Address Count	This is the number of IPv6 addresses and prefixes learned using the IPv6 snooping policy. Note: The maximum limit address count is the maximum size of the IPv6 source guard binding table. At the time of writing, it is 50 for the GS2210 Switch series. See the product datasheet for the latest specifications.
Add	Click this to create the IPv6 source guard policy or to update an existing one.
Cancel	Click this to reset the values above or if not applicable, to clear the fields above.

Table 139 Advanced Application > IP Source Guard > IPv6 Snooping Policy Setup (Standalone mode)

LABEL	DESCRIPTION
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each IPv6 snooping policy.
Name	This field displays the descriptive name for identification purposes for this IPv6 source guard policy.
Protocol	This field displays the protocols learned from DHCPv6 sniffed packets.
Prefix Glean	This field displays the IPv6 prefixes learned from DHCPv6 sniffed packets.
Limit Address Count	This field displays the the number of IPv6 addresses and prefixes learned using the IPv6 snooping policy.
Delete	Select an entry checkbox and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

25.15 IPv6 Snooping VLAN Setup

Use this screen to enable a DHCPv6 snooping policy on a specific VLAN interface. To open this screen, click **Advanced Application > IP Source Guard > IPv6 Snooping VLAN Setup**.

Figure 204 Advanced Application > IP Source Guard > IPv6 Snooping VLAN Setup (Standalone mode)

The following table describes the labels in this screen.

Table 140 Advanced Application > IP Source Guard > IPv6 Snooping VLAN Setup (Standalone mode)

LABEL	DESCRIPTION
Interface	Select the VLAN interface to apply the selected DHCPv6 snooping policy.
Policy	Select the IPv6 snooping policy to apply to this VLAN interface.
Add	Click this to create the IPv6 source guard policy or to update an existing one.
Cancel	Click this to reset the values above 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.
Interface	This field displays the VLAN interface.
Policy	This field displays the DHCPv6 snooping policy.

Table 140 Advanced Application > IP Source Guard > IPv6 Snooping VLAN Setup (Standalone mode)

LABEL	DESCRIPTION
Delete	Select an entry checkbox and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

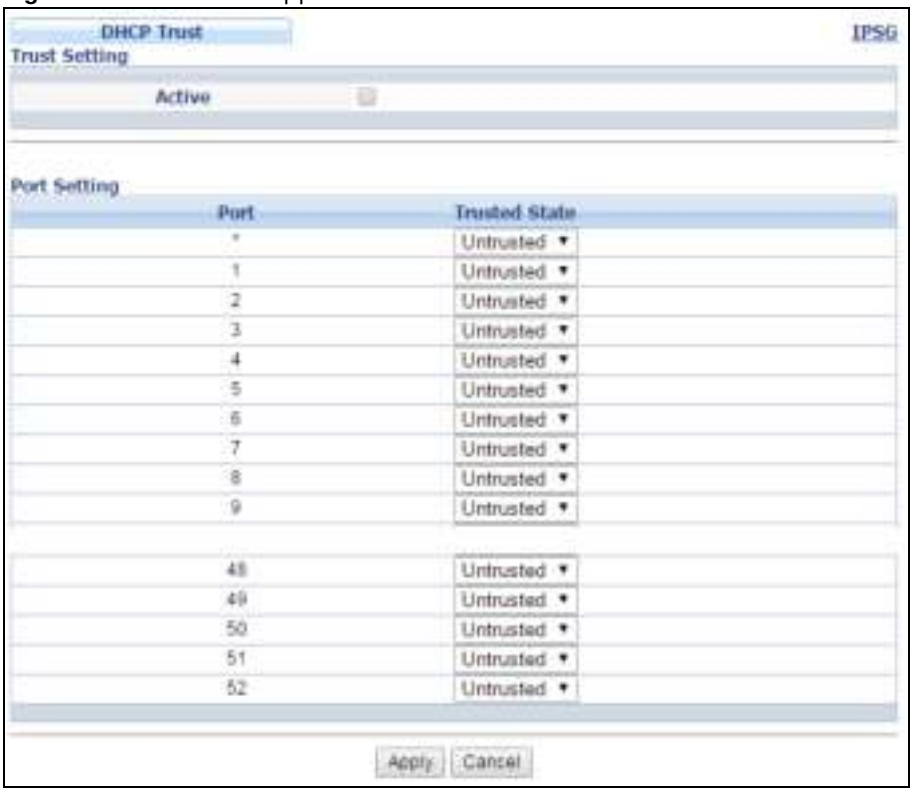
25.16 IPv6 DHCP Trust Setup

Use this screen to specify which ports are trusted for DHCPv6 snooping. To open this screen, click **Advanced Application > IP Source Guard > IPv6 DHCP Trust Setup**.

Note: DHCPv6 solicit packets are sent from a DHCPv6 client to a DHCPv6 server. Reply packets from a DHCPv6 server connected to an untrusted port are discarded.

Use port * to have all ports be **Untrusted** or **Trusted**.

Figure 205 Advanced Application > IP Source Guard > IPv6 DHCP Trust Setup (Standalone mode)



The following table describes the labels in this screen.

Table 141 Advanced Application > IP Source Guard > IPv6 DHCP Trust Setup (Standalone mode)

LABEL	DESCRIPTION
Active	Select this to specify whether ports are trusted or untrusted ports for DHCP snooping. If you do not select this then **IPv6 DHCP Trust** is not used and all ports are automatically trusted.
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 (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are connected to DHCPv6 servers or other switches. Untrusted ports are connected to subscribers, and the Switch discards DHCPv6 packets from untrusted ports in the following situations: • The packet is a DHCPv6 server packet (for example, ADVERTISE, REPLY, or RELAY-REPLY). • The source MAC address and source IP address in the packet do not match any of the current bindings.
Apply	Click **Apply** 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 **Save** 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.

25.17 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

25.17.1 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.

25.17.1.1 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: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

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.

25.17.1.2 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 206 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.

25.17.1.3 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 43 on page 413 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 43 on page 413).

25.17.1.4 Configuring DHCP Snooping

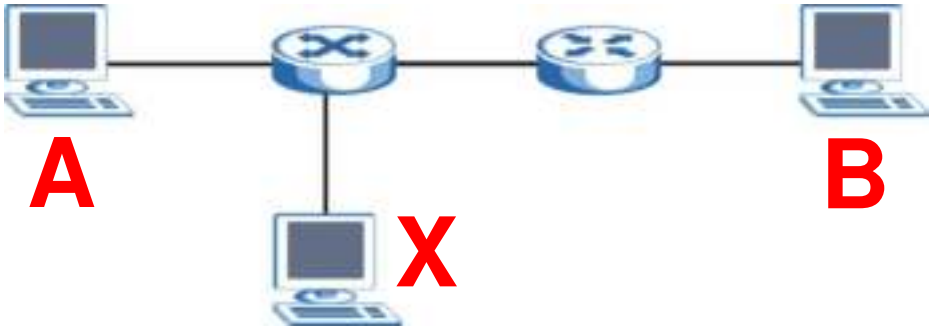
Follow these steps to configure DHCP snooping on the Switch.

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.

25.17.2 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 207 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.

25.17.2.1 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 10 on page 130).

- 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.

25.17.2.2 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.

25.17.2.3 Syslog

The Switch can send syslog messages to the specified syslog server (Chapter 50 on page 485) 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.

25.17.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1. Configure DHCP snooping. See Section 25.17.1.4 on page 297.

   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

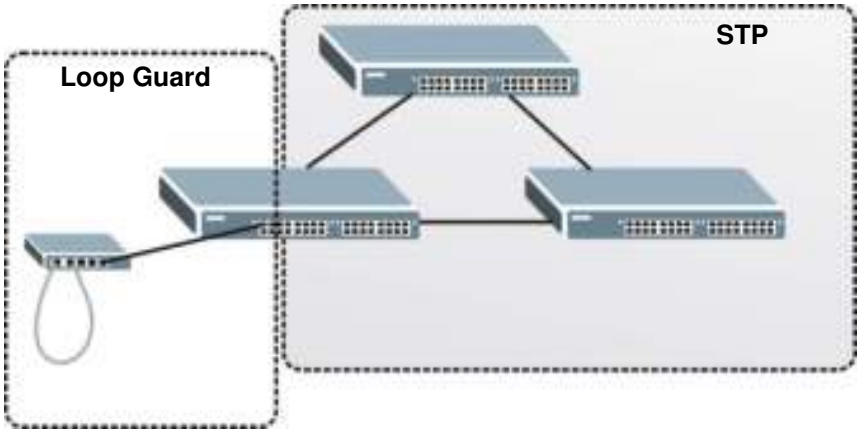
Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

26.1 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 208 Loop Guard vs STP



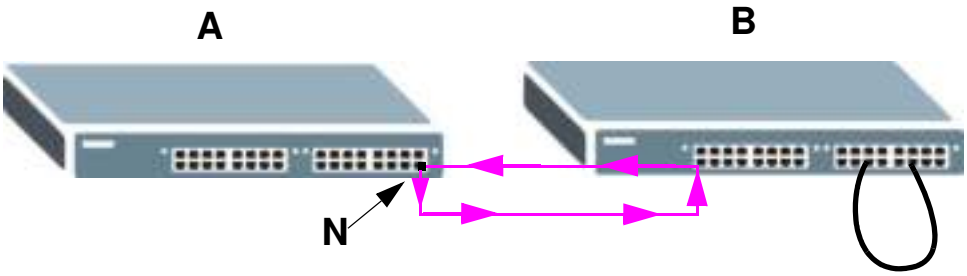
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends 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 switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

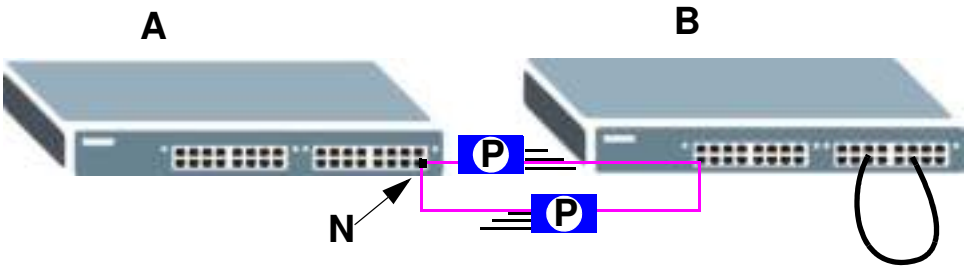
Figure 209 Switch in Loop State



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.

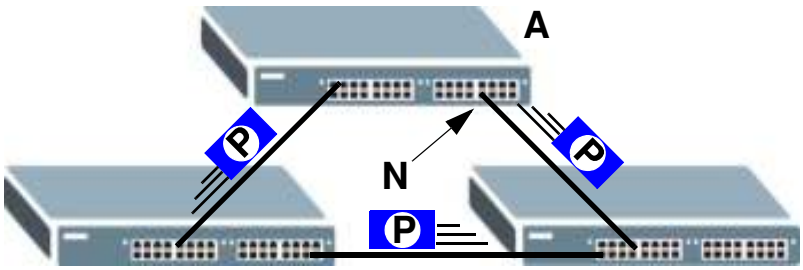
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 210 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 three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 211 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 6.6 on page 69) or via commands (see the Ethernet Switch CLI Reference Guide).

26.2 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 212 Advanced Application > Loop Guard (Standalone mode)

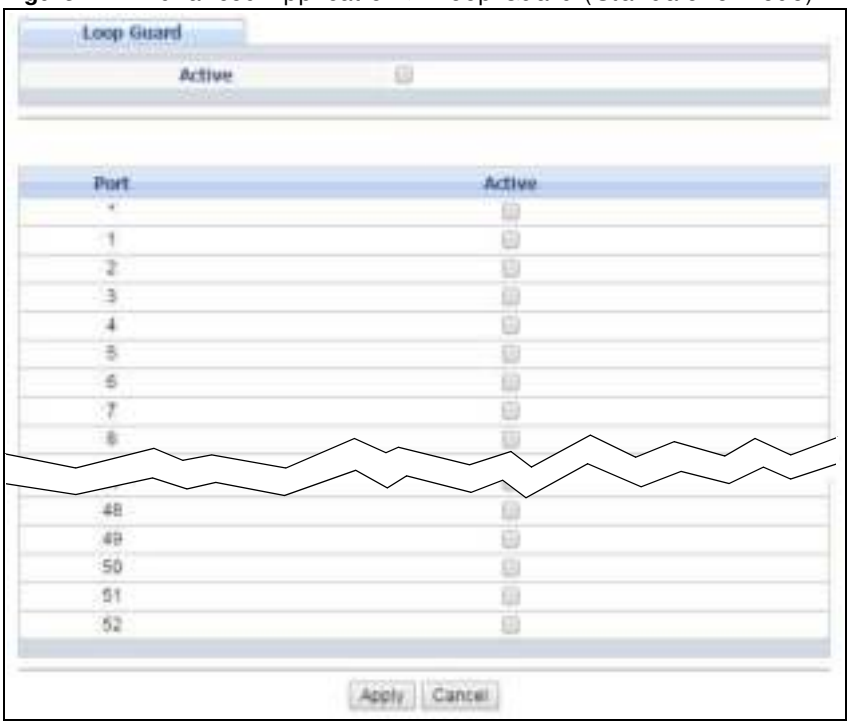
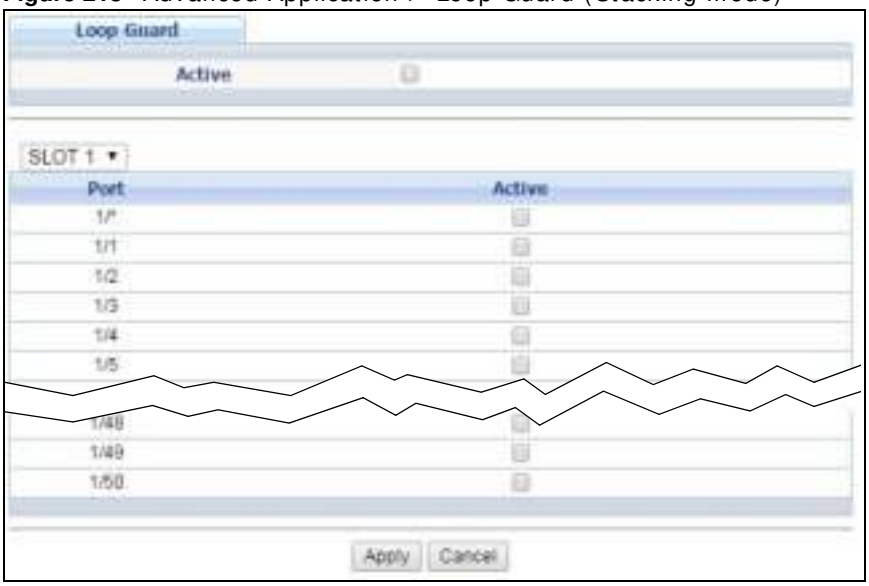


Figure 213 Advanced Application > Loop Guard (Stacking mode)



The following table describes the labels in this screen.

Table 142 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Active	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 is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

27

VLAN Mapping

This chapter shows you how to configure VLAN mapping on the Switch.

27.1 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.

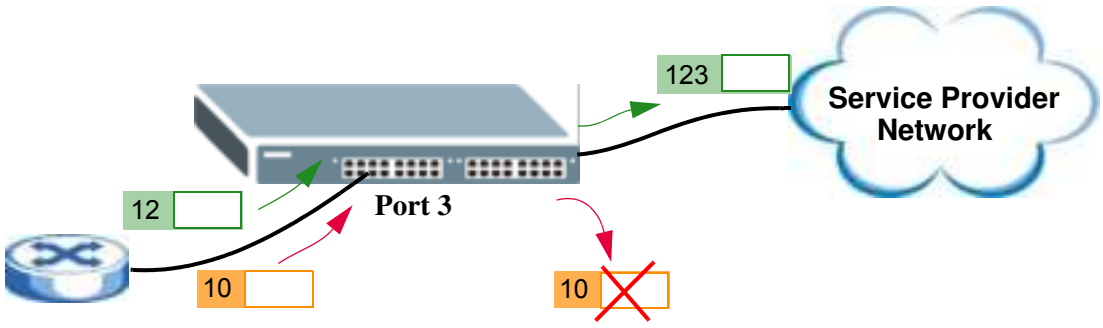
The Switch checks incoming traffic from the switch ports (non-management ports) against the VLAN mapping table first, the MAC learning table and then the VLAN table before forwarding them through the Gigabit uplink port. When VLAN mapping is enabled, the Switch discards the tagged packets that do not 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.

27.1.1 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 packets carrying a VLAN tag other than 12 (such as 10) and received on port 3 will be dropped.

Figure 214 VLAN mapping example



27.2 Enabling VLAN Mapping

Click **Advanced Application** and then **VLAN Mapping** in the navigation panel to display the screen as shown.

Figure 215 VLAN Mapping (Standalone mode)

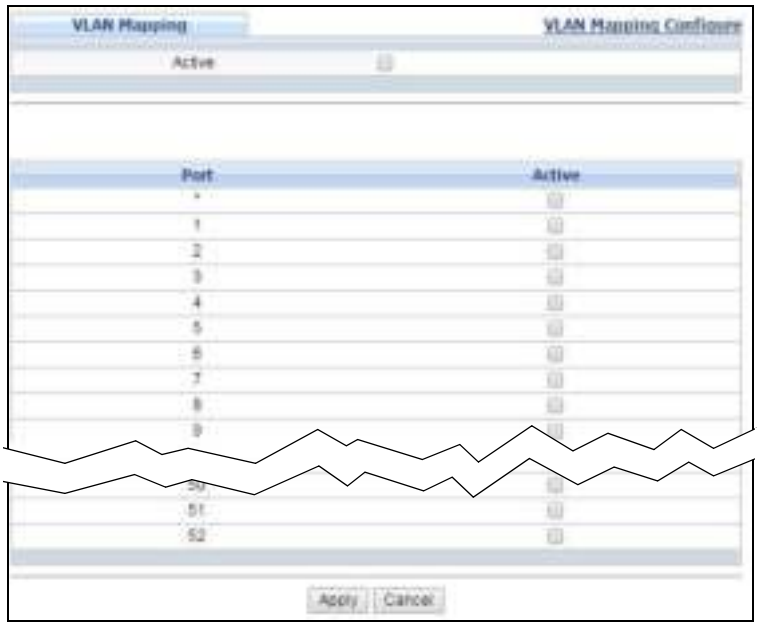


Figure 216 VLAN Mapping (Stacking mode)

The following table describes the labels in this screen.

Table 143 VLAN Mapping

LABEL	DESCRIPTION
Active	Select this option to enable VLAN mapping on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.

Table 143 VLAN Mapping (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable the VLAN mapping feature on this port. Clear this check box to disable the VLAN mapping feature.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

27.3 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 217 VLAN Mapping Configuration (Standalone mode)

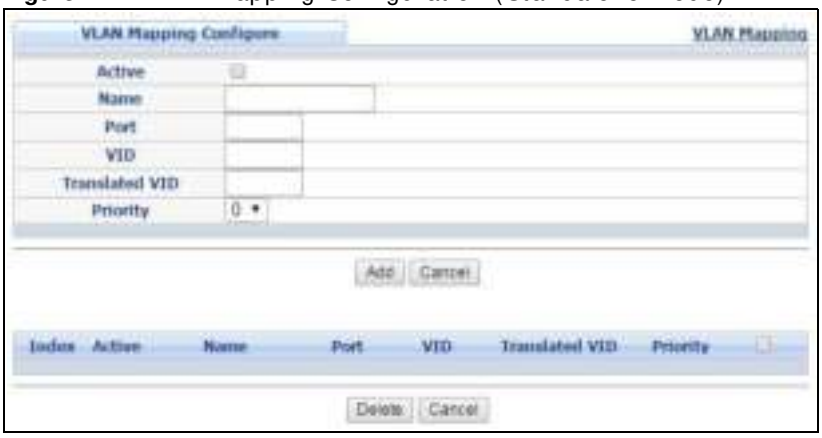
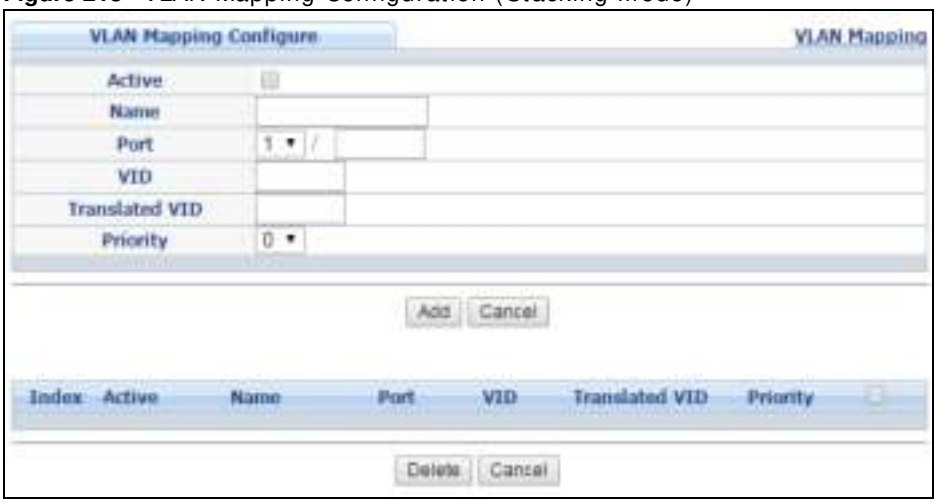


Figure 218 VLAN Mapping Configuration (Stacking mode)



The following table describes the labels in this screen.

Table 144 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. For stacking mode, the first field is the slot ID, the second field is the port number.
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 **Translated VID** 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.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This is the number of the VLAN mapping entry in the table. Click on an index number to change the settings.
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. In stacking mode, the first number represents the slot and the second the port number.
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.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

28

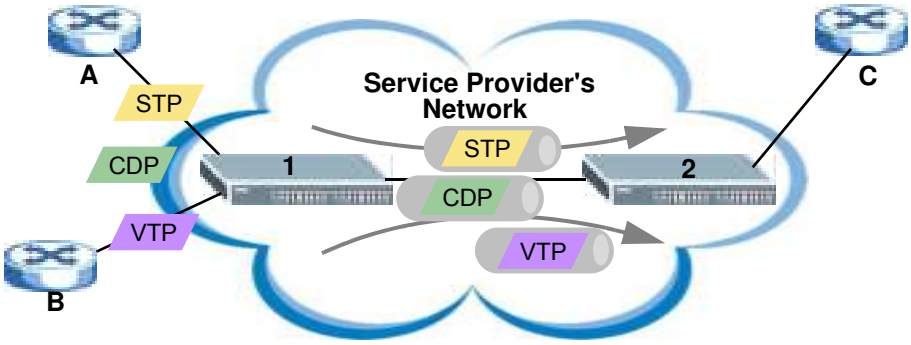
Layer 2 Protocol Tunneling

This chapter shows you how to configure layer-2 protocol tunneling on the Switch.

28.1 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.

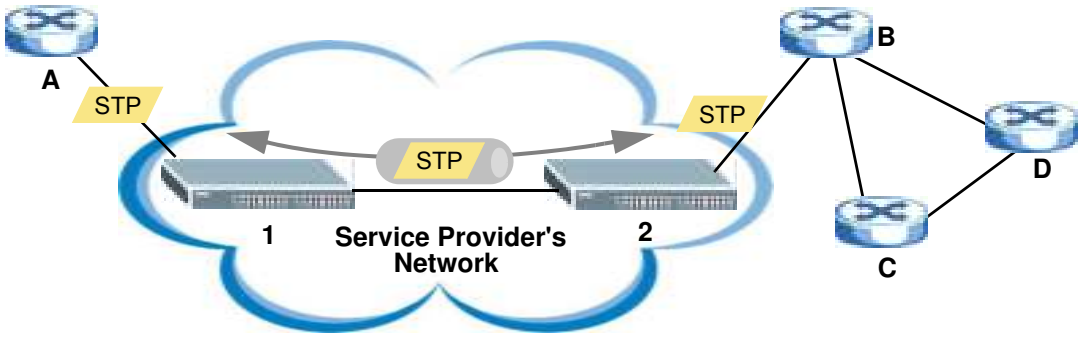
Figure 219 Layer-2 Protocol Tunneling Network Scenario



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 220 L2PT Network Example



28.1.1 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 220 on page 308) 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.

28.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application** > **Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 221 Advanced Application > Layer 2 Protocol Tunneling (Standalone mode)

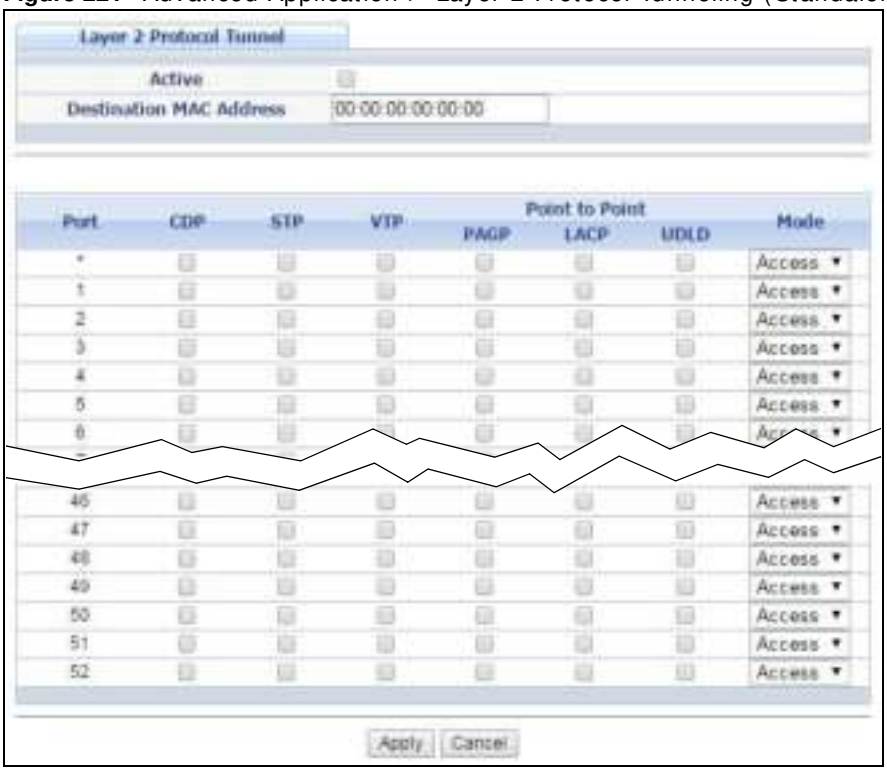
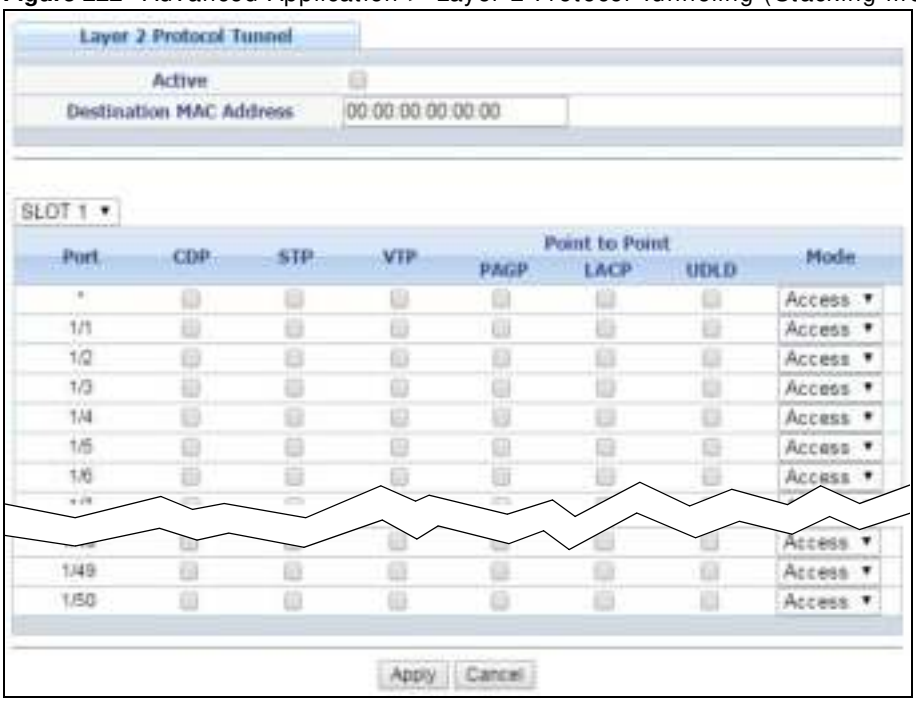


Figure 222 Advanced Application > Layer 2 Protocol Tunneling (Stacking mode)



The following table describes the labels in this screen.

Table 145 Advanced Application > 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.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
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	The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. 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.
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	Select **Access** to have the Switch encapsulate the incoming layer-2 protocol packets and forward them to the tunnel port(s). Select **Access** for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only. Select **Tunnel** 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.

Table 145 Advanced Application > Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29

sFlow

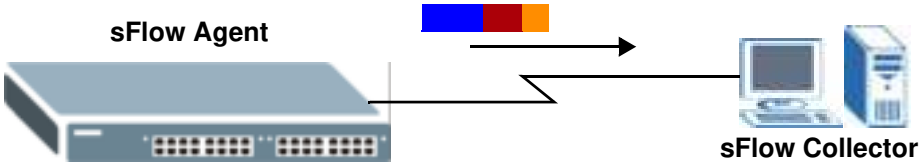
This chapter shows you how to configure sFlow to have the Switch monitor traffic in a network and send information to an sFlow collector for analysis.

29.1 sFlow Overview

sFlow (RFC 3176) is a standard technology for monitoring switched networks. An sFlow agent embedded on a switch or router gets sample data and packet statistics from traffic forwarded through its ports. The sFlow agent then creates sFlow data and sends it to an sFlow collector. The sFlow collector is a server that collects and analyzes sFlow datagram. An sFlow datagram includes packet header, input and output interface, sampling process parameters and forwarding information.

sFlow minimizes impact on CPU load of the Switch as it analyzes sample data only. sFlow can continuously monitor network traffic and create reports for network performance analysis and troubleshooting. For example, you can use it to know which IP address or which type of traffic caused network congestion.

Figure 223 sFlow Application



29.2 sFlow Port Configuration

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

Figure 224 Advanced Application > sFlow (Standalone mode)

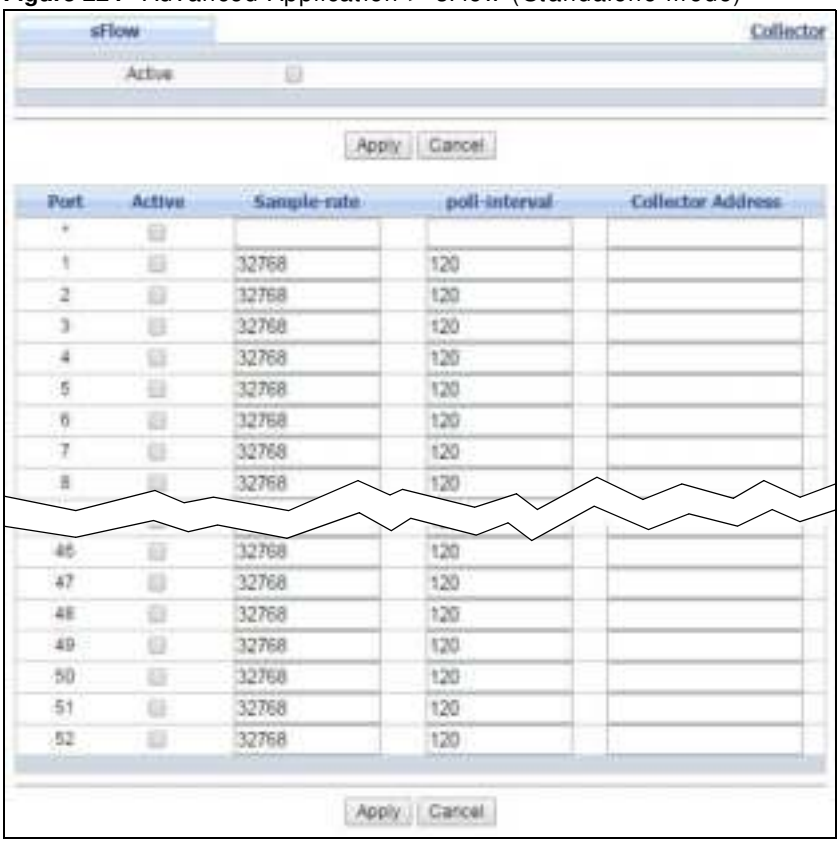
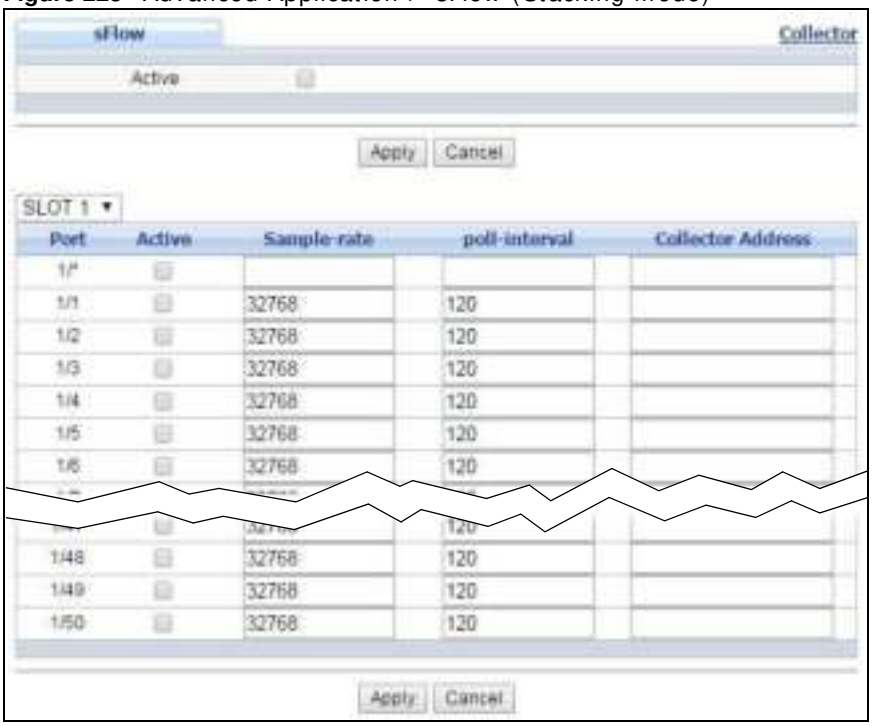


Figure 225 Advanced Application > sFlow (Stacking mode)



The following table describes the labels in this screen.

Table 146 Advanced Application > sFlow

LABEL	DESCRIPTION
Active	Select this to enable the sFlow agent on the Switch.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Active	Select this to allow the Switch to monitor traffic on this port and generate and send sFlow datagram to the specified collector.
Sample-rate	Enter a number (N) from 256 to 65535. The Switch captures every one out of N packets for this port and creates sFlow datagram.
poll-interval	Specify a time interval (from 20 to 120 in seconds) the Switch waits before sending the sFlow datagram and packet counters for this port to the collector.
Collector Address	Enter the IP address of the sFlow collector. Note: You must have the sFlow collector already configured in the **sFlow > Collector** screen. The sFlow collector does not need to be in the same subnet as the Switch, but it must be accessible from the Switch. Note: Configure UDP port 6343 (the default) on a NAT router to allow port forwarding if the collector is behind a NAT router. Configure a firewall rule for UDP port 6343 (the default) to allow incoming traffic if the collector is behind a firewall.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29.2.1 sFlow Collector Configuration

Click the **Collector** link in the **sFlow** screen to display the screen as shown. You can configure up to four sFlow collectors in this screen. You may want to configure more than one collector if the traffic load to be monitored is more than one collector can manage.

Figure 226 Advanced Application > sFlow > Collector

The following table describes the labels in this screen.

Table 147 Advanced Application > sFlow > Collector

LABEL	DESCRIPTION
Collector Address	Enter the IP address of the sFlow collector.
UDP Port	Enter a UDP port number the Switch uses to send sFlow datagram to the collector. If you change the port here, make sure you change it on the collector, too. The default port is 6343.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays the index number of this entry. Click on an index number to change the settings.
Collector Address	This field displays IP address of the sFlow collector.
UDP Port	This field displays port number the Switch uses to send sFlow datagram to the collector.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

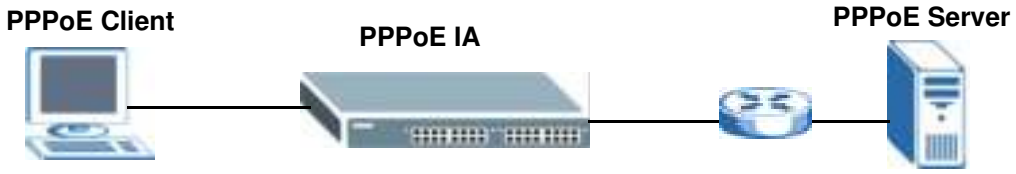
30

PPPoE

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.

30.1 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 on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



30.1.1 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 148 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.

30.1.2 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 149 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 150 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 takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, 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.

30.1.2.1 Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-option example is "Switch/07/0123" and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch's port 7 and belong to VLAN 123.

Table 151 PPPoE IA Circuit ID Sub-option Format: Using Identifier String and Variables

SubOpt	Length	Value						
0x01 (1 byte)	N (1 byte)	Identifier String (53 byte)	delimiter (1 byte)	Slot ID (1 byte)	delimiter (1 byte)	Port No (2 byte)	delimiter (1 byte)	VLAN ID (4 bytes)

30.1.2.2 WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE > Intermediate Agent** screen, 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 152 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)

30.1.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

30.2 The PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the Switch.

Click **Advanced Application** > **PPPoE** in the navigation panel to display the screen as shown. Click **Click Here** to go to the **Intermediate Agent** screen.

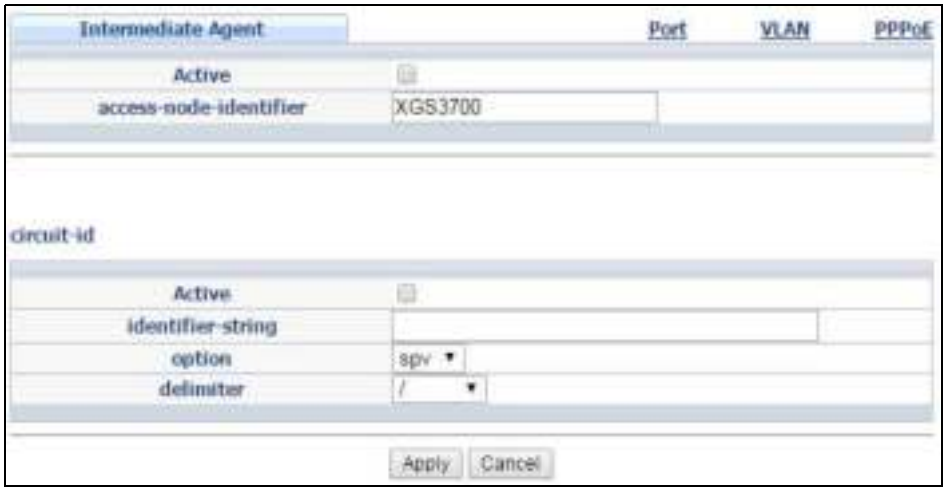
Figure 227 Advanced Application > PPPoE Intermediate Agent

30.3 PPPoE Intermediate Agent

Use this screen to configure the Switch to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **Advanced Application** > **PPPoE** > **Intermediate Agent** in the navigation panel to display the screen as shown.

Figure 228 Advanced Application > PPPoE > Intermediate Agent



The following table describes the labels in this screen.

Table 153 Advanced Application > PPPoE > Intermediate Agent

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the Switch.
access-node-identifier	Enter up to 20 ASCII characters to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.
circuit-id	Use this section to configure the Circuit ID field in the PADI and PADR packets. The Circuit ID you configure for a specific port or for a specific VLAN on a port has priority over this. The Circuit ID you configure for a specific port (in the **Advanced Application > PPPoE > Intermediate Agent > Port** screen) or for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has priority over this. That means, if you also want to configure PPPoE IA Per-Port or Per-Port Per-VLAN setting, leave the fields here empty and configure circuit-id and remote-id in the Per-Port or Per-Port Per-VLAN screen.
Active	Select this option to have the Switch add the user-defined identifier string and variables (specified in the **option** 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 the string specified in the **access-node-identifier** field.
identifier-string	Specify a string that the Switch adds in the Agent Circuit ID sub-option. You can enter up to 53 ASCII characters. Spaces are allowed.
option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include **sp**, **sv**, **pv** and **spv** which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value.
delimiter	Select a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. You can use a pound key (**#**), semi-colon (**;**), period (**.**), comma (**,**), forward slash (**/**) or space.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.3.1 PPPoE IA Per-Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The Switch will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the Switch and there are no trusted ports.

Click the **Port** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 229 Advanced Application > PPPoE > Intermediate Agent > Port (Standalone mode)

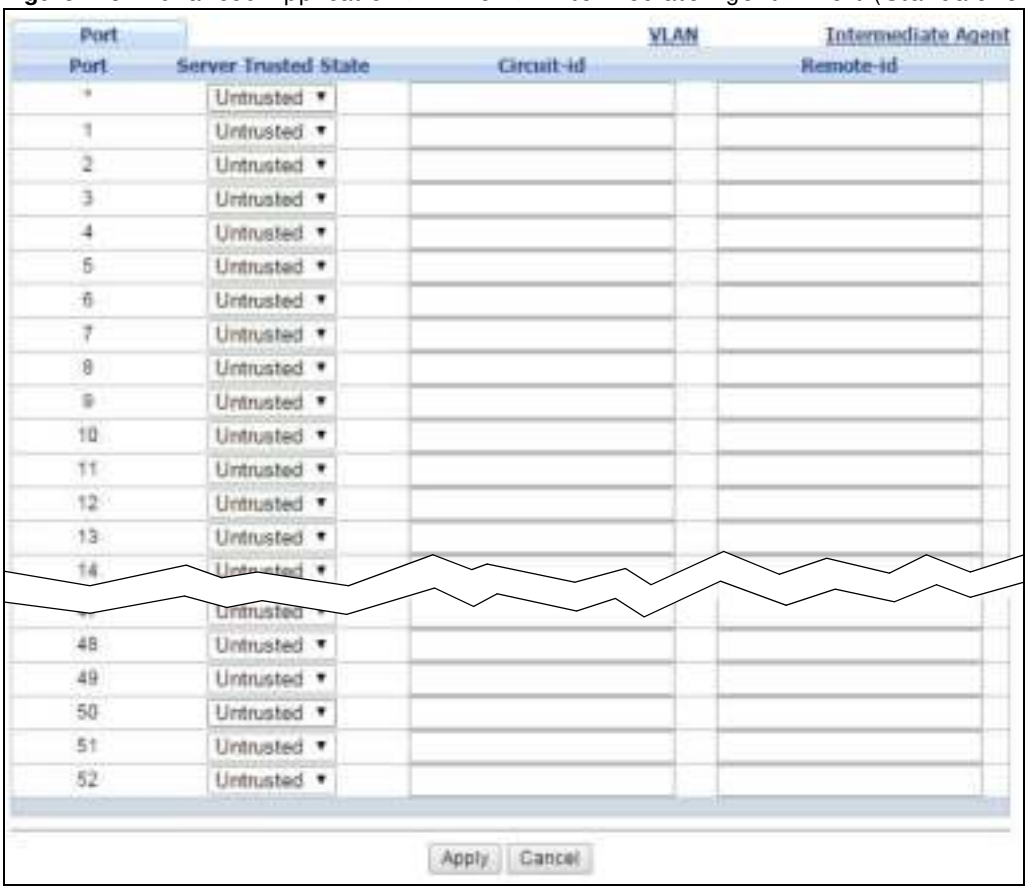
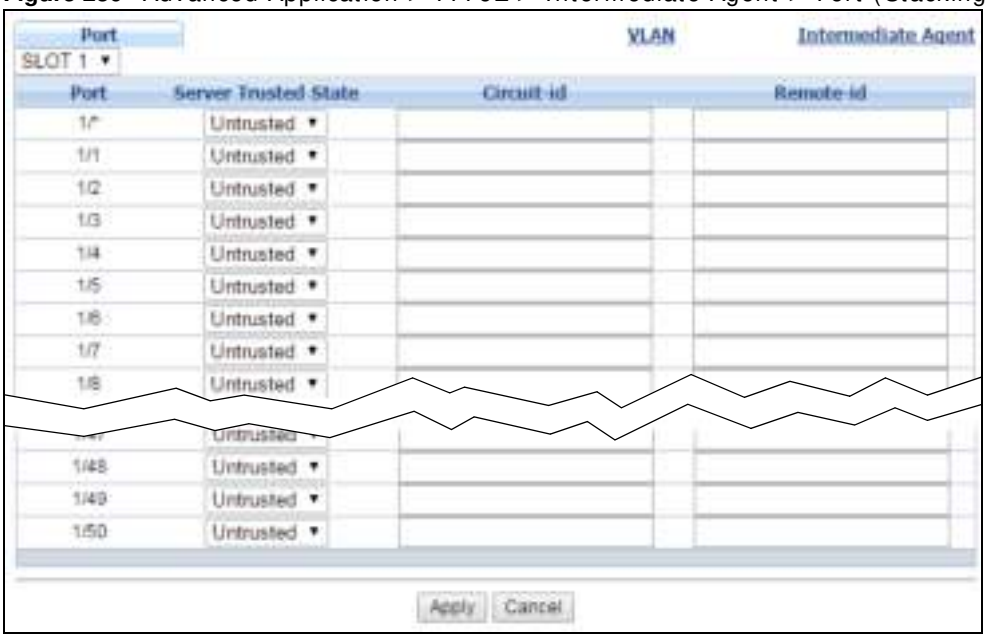


Figure 230 Advanced Application > PPPoE > Intermediate Agent > Port (Stacking mode)



The following table describes the labels in this screen.

Table 154 Advanced Application > PPPoE > Intermediate Agent > Port

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is 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.
Server Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are uplink ports connected to PPPoE servers. • If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. • If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. • If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). • The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.

Table 154 Advanced Application > PPPoE > Intermediate Agent > Port (continued)

LABEL	DESCRIPTION
Remote-id	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. If you do not specify a string here or in the **Remote-id** field for a VLAN on a port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.3.2 PPPoE IA Per-Port Per-VLAN

Use this screen to configure PPPoE IA settings that apply to a specific VLAN on a port.

Click the **VLAN** link in the **Intermediate Agent > Port** screen to display the screen as shown.

Figure 231 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN (Standalone mode)

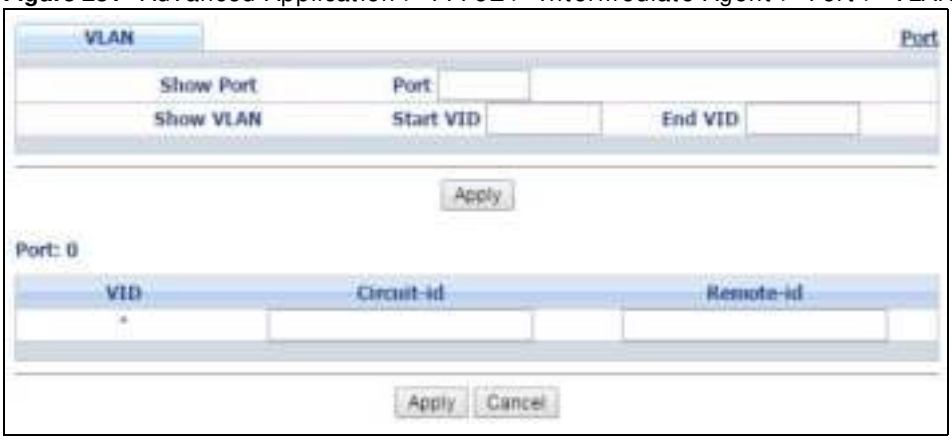
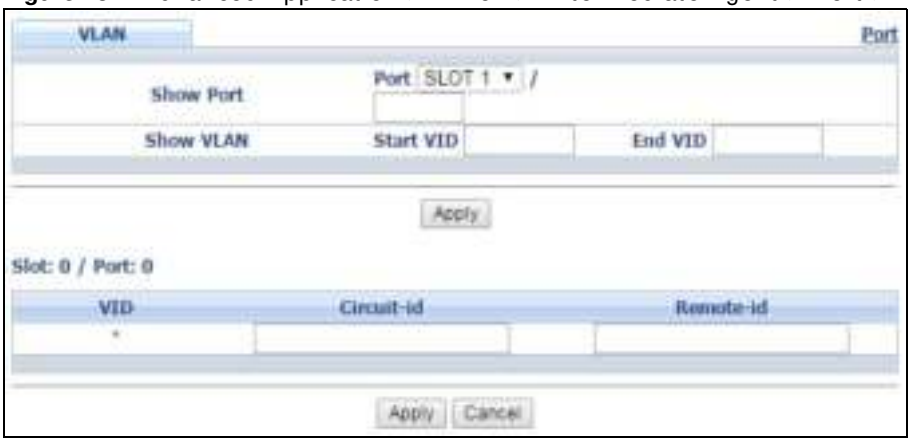


Figure 232 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN (Stacking mode)



The following table describes the labels in this screen.

Table 155 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

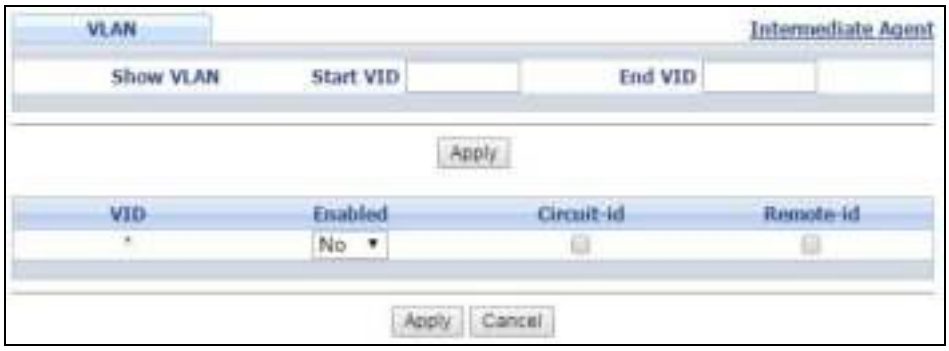
LABEL	DESCRIPTION
Show Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLAN(s) on the port. For Stacking mode, the first field box is the Slot ID, the second field box is the port.
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Slot / Port	For Stacking mode, the first field box displaysa the Slot ID, the second field box displays the port number.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
Port	This field displays the port number specified above.
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.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for this VLAN on the specified port. Spaces are allowed. If you do not specify a string here or in the **Remote-id** field for a specific port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure here has the highest priority.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.3.3 PPPoE IA for VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the Switch appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click the **VLAN** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 233 Advanced Application > PPPoE > Intermediate Agent > VLAN



The following table describes the labels in this screen.

Table 156 Advanced Application > PPPoE > Intermediate Agent > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** 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.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-id	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-id	Select this option to make the Remote ID settings for a specific VLAN take effect.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31

Error Disable

31.1 Error Disable Overview

This chapter shows you how to configure the rate limit for control packets on a port, and set the Switch to take an action (such as to shut down a port or stop sending packets) on a port when the Switch detects a pre-configured error. It also shows you how to configure the Switch to automatically undo the action after the error is gone.

31.1.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

31.1.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator or the commands. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

31.1.3 What You Can Do

- Use the **Errdisable Status** screen (Section 31.3 on page 326) to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information.
- Use the **CPU Protection** screen (Section 31.4 on page 328) to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
- Use the **Errdisable Detect** screen (Section 31.5 on page 330) to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
- Use the **Errdisable Recovery** screen (Section 31.6 on page 331) to set the Switch to automatically undo an action after the error is gone.

31.2 The Error Disable Screen

Use this screen to configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

Figure 234 Advanced Application > Errdisable

The following table describes the labels in this screen.

Table 157 Advanced Application > Errdisable

LABEL	DESCRIPTION
Errdisable Status	Click this link to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information.
CPU protection	Click this link to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
Errdisable Detect	Click this link to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
Errdisable Recovery	Click this link to set the Switch to automatically undo an action after the error is gone.

31.3 Error-Disable Status

Use this screen to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information. Click the **Click here** link next to **Errdisable Status** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 235 Advanced Application > Errdisable > Errdisable Status (Standalone mode)

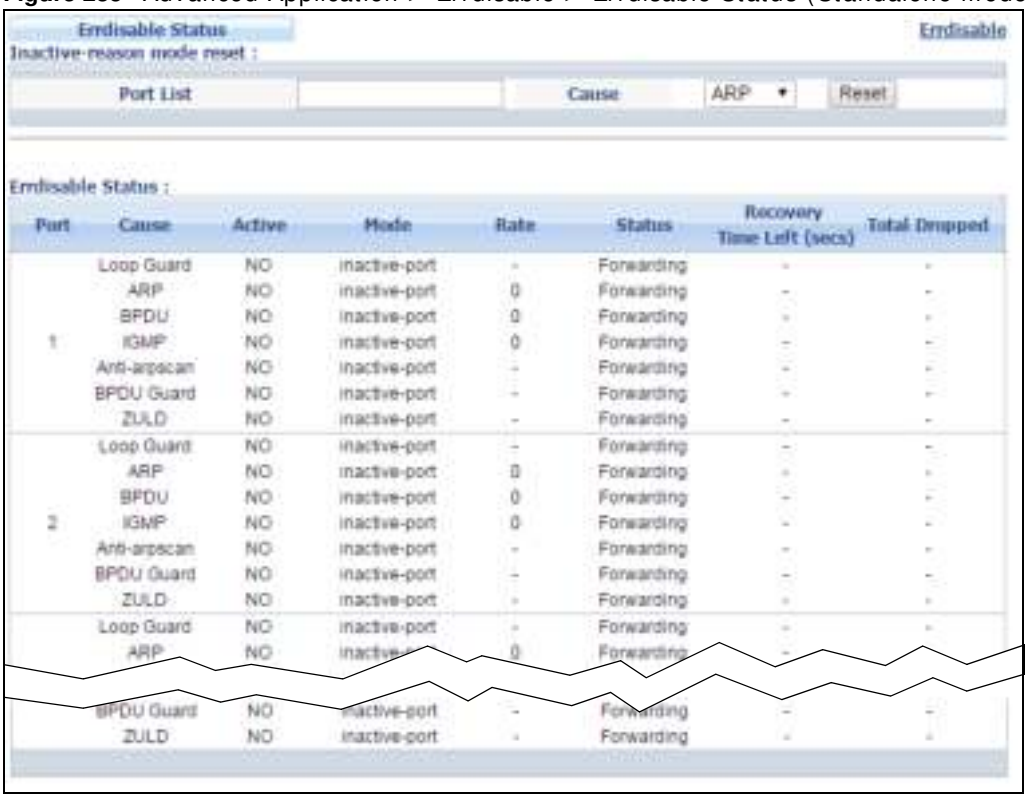
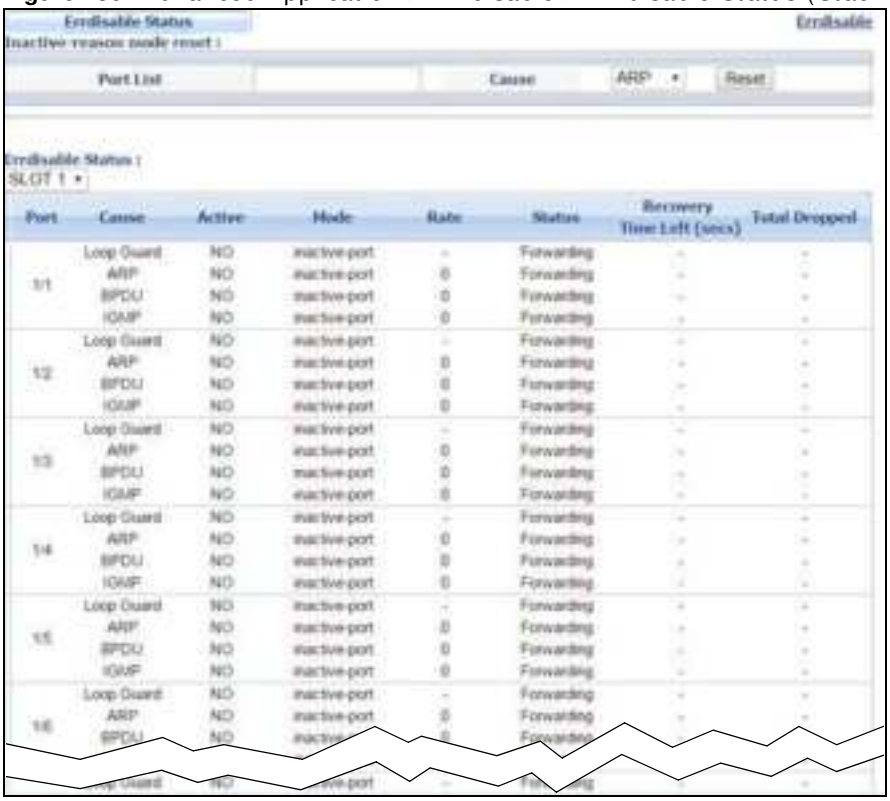


Figure 236 Advanced Application > Errdisable > Errdisable Status (Stacking mode)



The following table describes the labels in this screen.

Table 158 Advanced Application > Errdisable > Errdisable Status

LABEL	DESCRIPTION
Inactive-reason mode reset	
Port List	Enter the number of the port(s) (separated by a comma) on which you want to reset inactive-reason status. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Cause	Select the cause of inactive-reason mode you want to reset here.
Reset	Press to reset the specified port(s) to handle ARP, BPDU or IGMP packets instead of ignoring them, if the port(s) is in inactive-reason mode.
Errdisable Status	
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
Cause	This displays the type of the control packet received on the port or the feature enabled on the port and cause the Switch to take the specified action.
Active	This field displays whether the control packets (ARP, BPDU, and/or IGMP), on the port is being detected or not. It also shows whether loop guard, anti-arp scanning, BPDU guard or ZULD is enabled on the port.
Mode	This field shows the action that the Switch takes for the cause. • **inactive-port** - The Switch disables the port. • **inactive-reason** - The Switch drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** - The Switch drops the additional control packets the port(s) has to handle in every one second.
Rate	This field displays how many control packets this port can receive or transmit per second. It can be adjusted in CPU Protection. **0** means no rate limit.
Status	This field displays the errdisable status • **Forwarding**: The Switch is forwarding packets. Rate-limitation mode is always in **Forwarding** status. • **Err-disable**: The Switch disables the port on which the control packets are received (inactive-port) or drops specified control packets on the port (inactive-reason)
Recovery Time Left (secs)	This field displays the time (seconds) left before the port(s) becomes active of Errdisable Recovery.
Total Dropped	This field displays the total packet number dropped by this port where the packet rate exceeds the rate of mode rate-limitation.

31.4 CPU Protection Configuration

Use this screen to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port. Click the **Click Here** link next to **CPU protection** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Note: After you configure this screen, make sure you also enable error detection for the specific control packets in the **Advanced Application** > **Errdisable** > **Errdisable Detect** screen.

Figure 237 Advanced Application > Errdisable > CPU protection (Standalone mode)

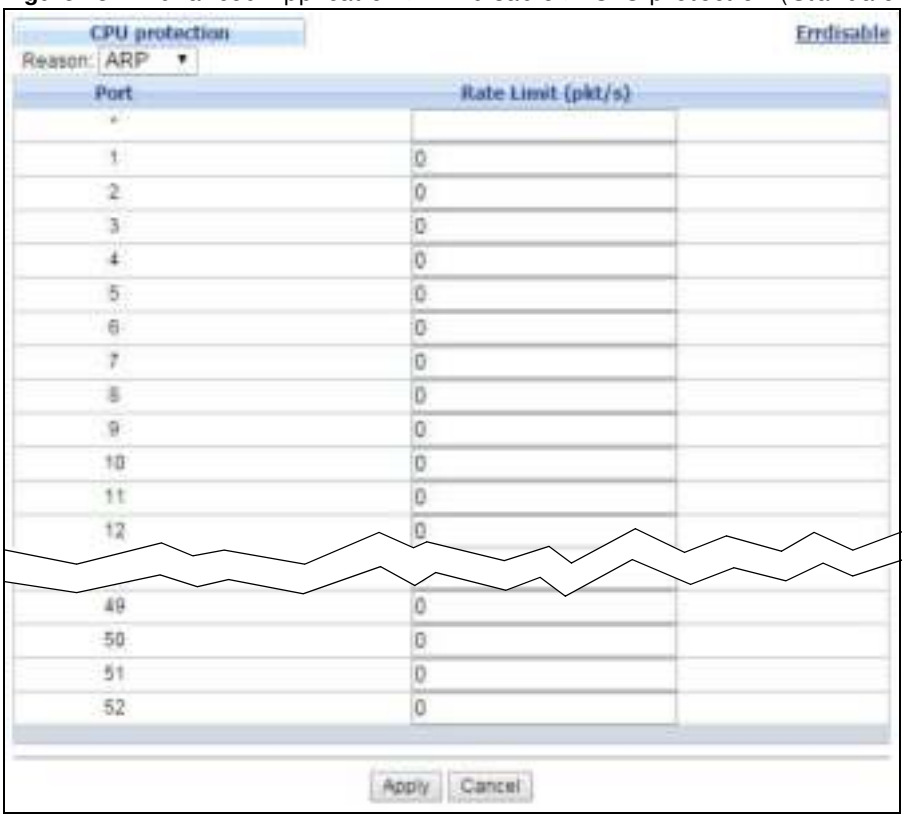
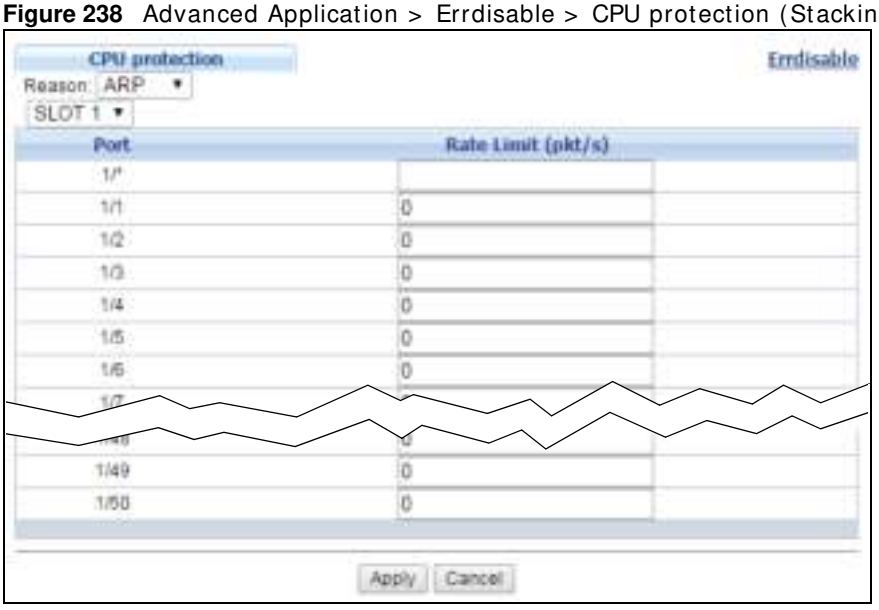


Figure 238 Advanced Application > Errdisable > CPU protection (Stacking mode)



The following table describes the labels in this screen.

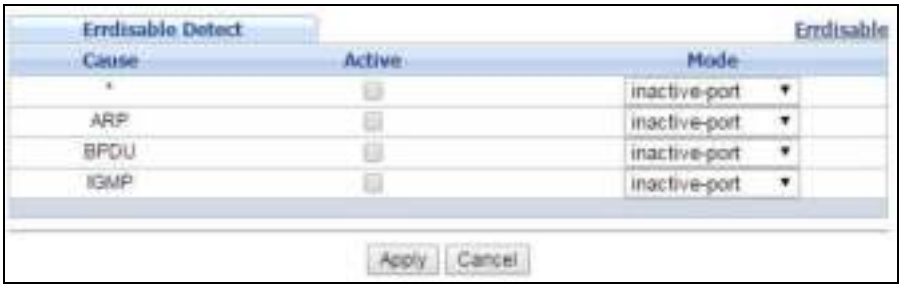
Table 159 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
1/*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. **0** means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. See Section 31.5 on page 330 for detailed information.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31.5 Error-Disable Detect Configuration

Use this screen to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click the **Click Here** link next to **Errdisable Detect** link in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 239 Advanced Application > Errdisable > Errdisable Detect



The following table describes the labels in this screen.

Table 160 Advanced Application > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the **Advanced Application > Errdisable > CPU protection** screen. • **inactive-port** - The Switch disables the port on which the control packets are received. • **inactive-reason** - The Switch bypasses the processing of the specified control packets (such as ARP or IGMP packets), or drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** - The Switch drops the additional control packets the port has to handle in every one second.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31.6 Error-Disable Recovery Configuration

Use this screen to configure the Switch to automatically undo an action after the error is gone. Click the **Click Here** link next to **Errdisable Recovery** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 240 Advanced Application > Errdisable > Errdisable Recovery (Standalone Mode)

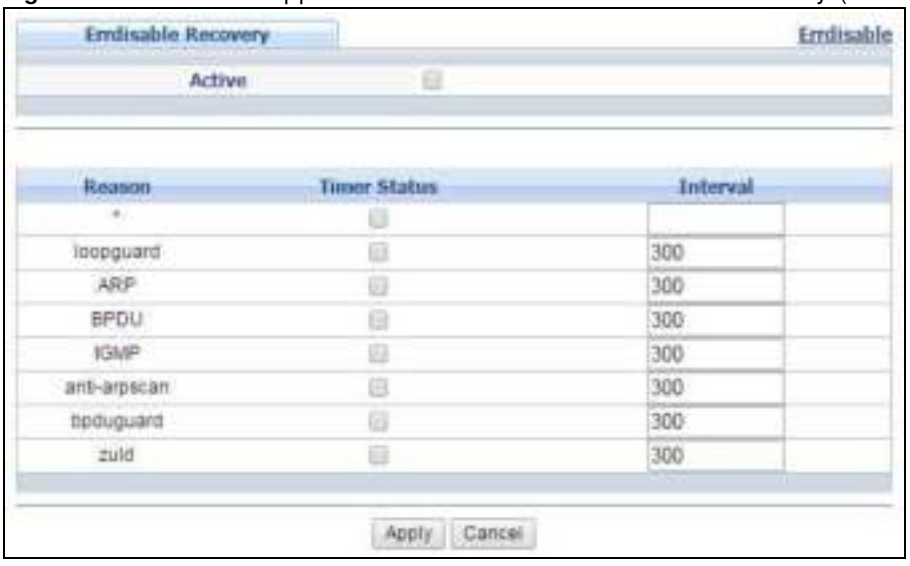
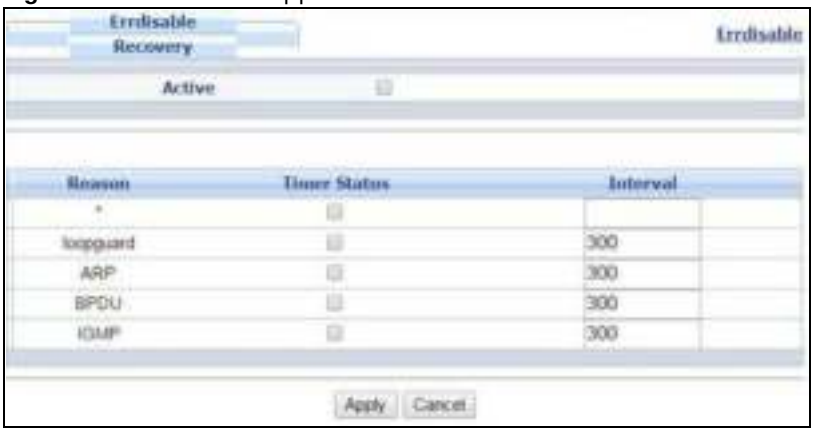


Figure 241 Advanced Application > Errdisable > Errdisable Recovery (Stacking Mode)



The following table describes the labels in this screen.

Table 161 Advanced Application > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Select this option to turn on the error-disable recovery function on the Switch.
Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.
Timer Status	Select this option to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32

MAC Pinning

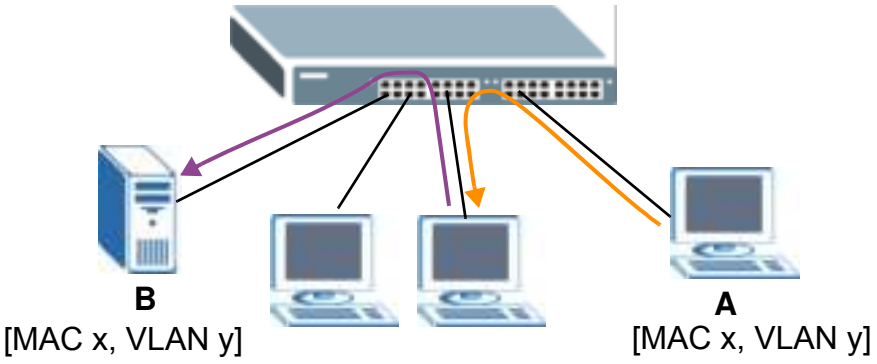
This chapter shows you how to configure MAC pinning on the Switch.

32.1 MAC Pinning Overview

When the Switch obtains a connected device's MAC address, it adds an entry in the MAC address forwarding table and uses the table to determine how to forward frames. In addition to the source MAC address of a received frame, the Switch also learns the VLAN to which the device belongs and the port on which the frame is received. If the Switch learns the same MAC address and same VLAN ID on another port, it updates the MAC address table immediately.

MAC pinning allows you to set a port or multiple ports to have priority over other ports in MAC address learning. That means when a MAC address (and VLAN ID) is learned on a MAC-pinning-enabled port, the MAC address will not be learned on any other port until the aging time for the dynamically learned MAC address in the table expires.

This helps enhance security. For example, when an attacker (**A**) sends packets to all connected clients by spoofing the source MAC address of a server (**B**) connected to one of the Switch's ports, on which MAC pinning is enabled, the responses from clients will still be forwarded to the server according to the Switch's MAC forwarding table.



32.2 MAC Pinning Configuration

Use this screen to enable MAC pinning on the Switch and on specific ports. Click **Advanced Application** > **MAC Pinning** in the navigation panel to open the following screen.

Figure 242 Advanced Application > MAC Pinning (Standalone mode)

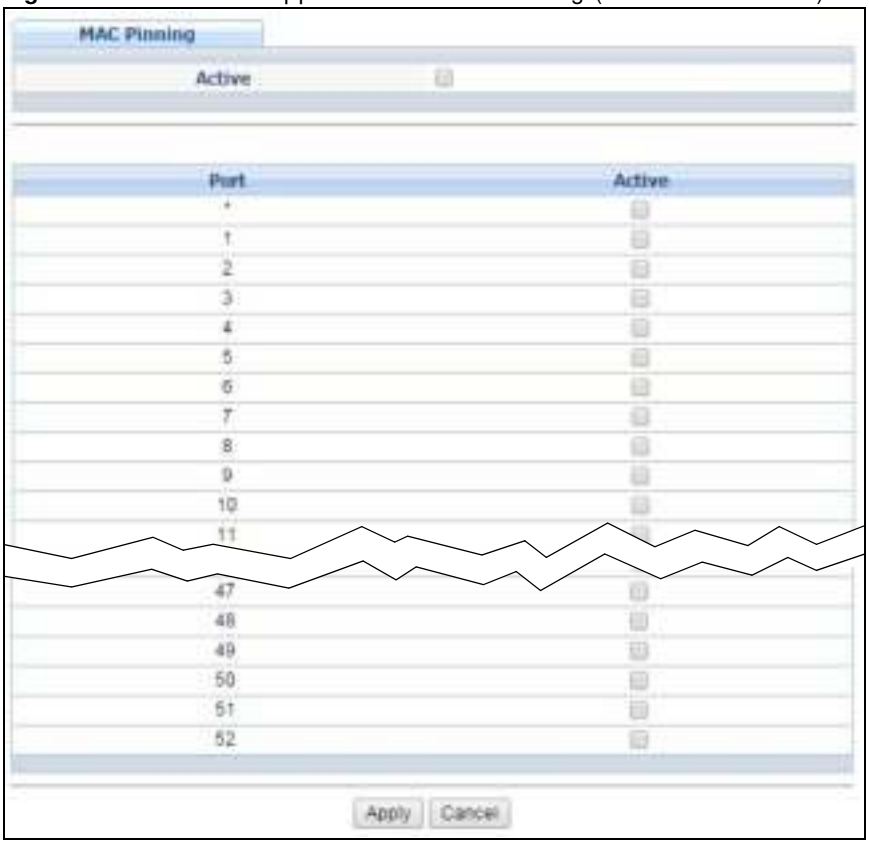
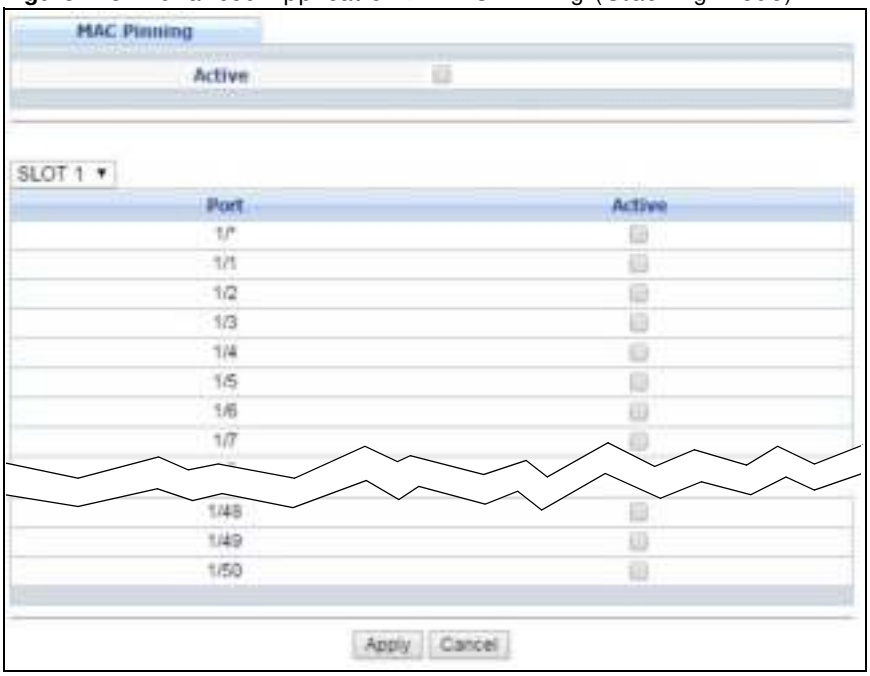


Figure 243 Advanced Application > MAC Pinning (Stacking mode)



The following table describes the labels in this screen.

Table 162 Advanced Application > MAC Pinning

LABEL	DESCRIPTION
Active	Select this option to turn on the MAC pinning function on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable MAC pinning on this port. The port then has priority over other ports in MAC address learning. Clear this check box to disable MAC pinning.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

33

Private VLAN

33.1 Private VLAN Overview

Use private VLAN if you want you to block traffic between ports in the same VLAN. **Community** and **Isolated** VLANs are secondary private VLANs that must be associated with a **Primary** private VLAN.

- **Primary**: Ports in a **Primary** VLAN are promiscuous and they can communicate with all promiscuous ports in the same primary VLAN, and all ports in associated community and isolated VLANs. They cannot communicate with ports in different primary VLANs.
- **Community**: Ports in a **Community** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in **Isolated** VLANs, non-associated **Primary** VLAN promiscuous ports nor community ports in different **Community** VLANs.
- **Isolated**: Ports in an **Isolated** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN only. They cannot communicate with other isolated ports in the same **Isolated** VLAN, non-associated **Primary** VLAN promiscuous ports nor any community ports.

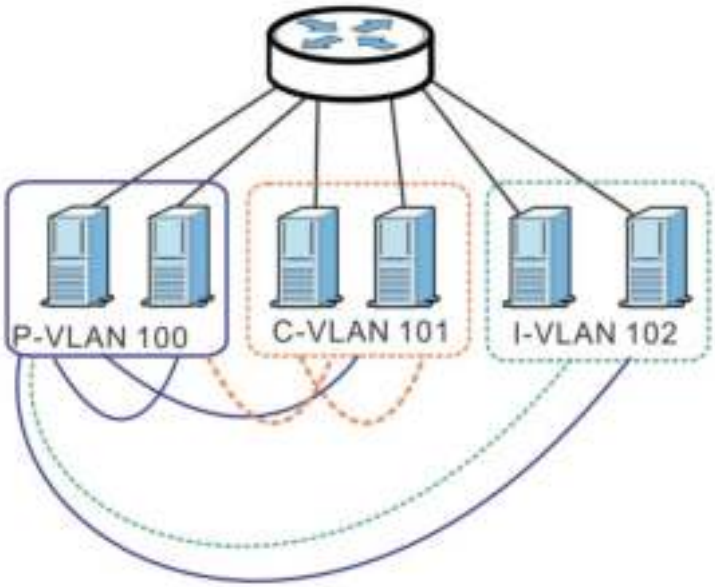


Table 163 PVLAN Graphic Key

LABEL	DESCRIPTION
P-VLAN 100	Primary private VLAN
C-VLAN 101	Community private VLAN
I-VLAN 102	Isolated private VLAN

Tagged Private VLANs can span switches but trunking ports must be VLAN-trunking ports - see **Advanced > VLAN > VLAN Port Setting**.

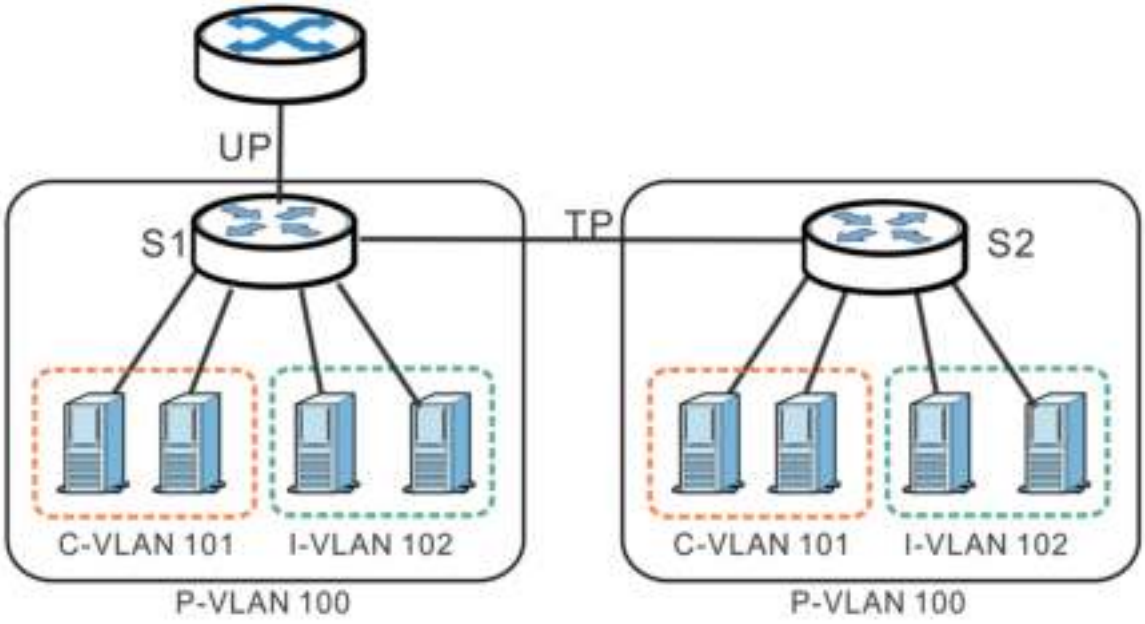


Table 164 Spanning PVLAN Graphic Key

LABEL	DESCRIPTION
UP	Uplink promiscuous port
TP	VLAN-trunking ports
S1, S2	Switch 1, Switch 2
P-VLAN 100	Primary private VLAN with VLAN ID tag of 100
C-VLAN 101	Community private VLAN with VLAN ID tag of 101
I-VLAN 102	Isolated private VLAN with VLAN ID tag of 102

This is the communication process if primary VLAN **P-VLAN 100** is associated with community VLAN **C-VLAN 101** and isolated VLAN **I-VLAN 102**.

- Promiscuous ports in **P-VLAN 100** can communicate with all ports in **P-VLAN 100** including community ports in **C-VLAN 101** and isolated ports in **I-VLAN 102**.
- Community ports in **C-VLAN 101** can communicate with promiscuous ports in **P-VLAN 100** and other community ports in **C-VLAN 101**. They cannot communicate with isolated ports in **I-VLAN 102**.
- Isolated ports can communicate with promiscuous ports in **P-VLAN 100**. They cannot communicate with other isolated ports in **I-VLAN 102** nor community ports in **C-VLAN 101**.

Note: **Isolation** in **VLAN > VLAN Port Setting** (see Section 7.7.2 on page 109) has a higher priority than private VLAN settings, so promiscuous ports with **Isolation** in **VLAN > VLAN Port Setting** enabled will not be able to communicate with each other.

33.1.1 Configuration

You must go to the **Static VLAN** screen first (see Section 7.7 on page 106) to create VLAN IDs for **Primary**, **Isolated** or **Community** VLANs.

Click **Advanced Application > Private VLAN** to display the following screen.

Figure 244 Advanced Application > Private VLAN (Standalone mode)

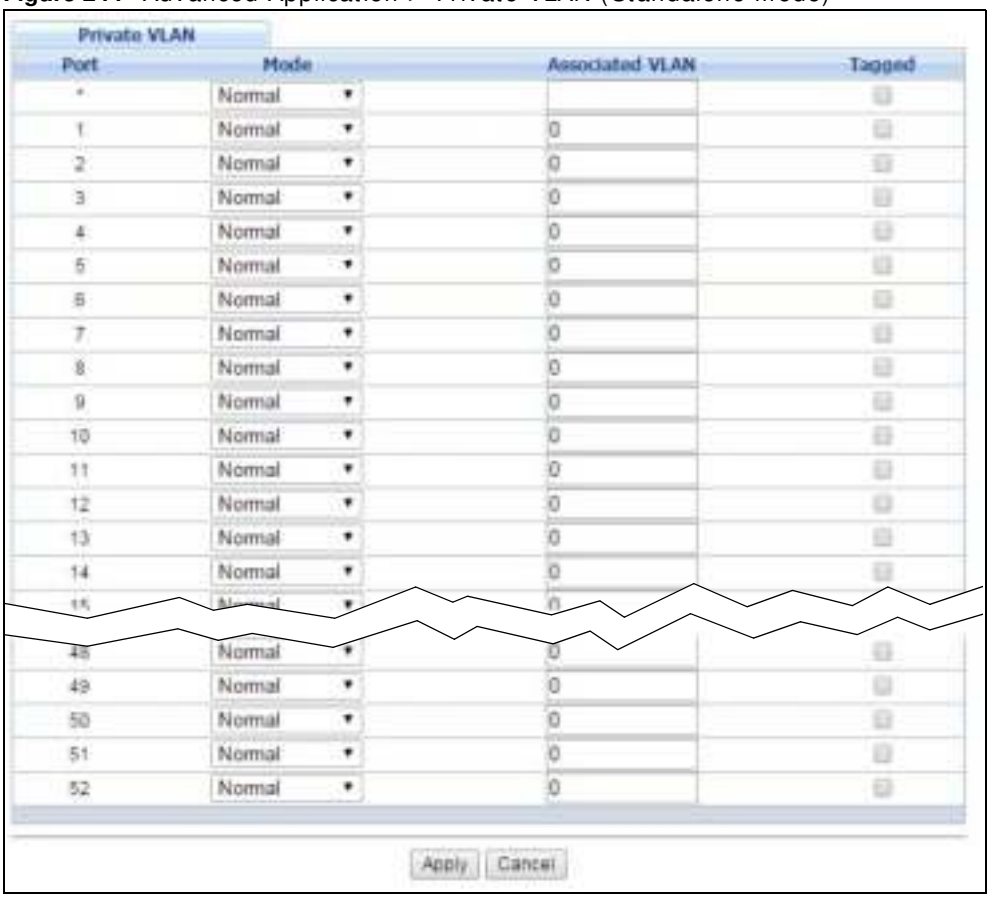
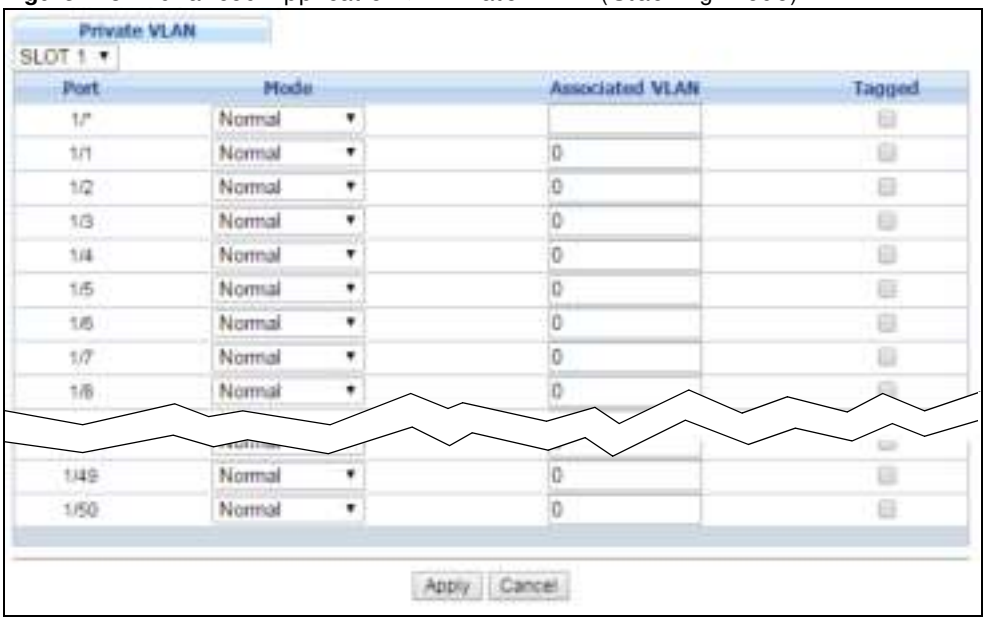


Figure 245 Advanced Application > Private VLAN (Stacking mode)



The following table describes the labels in this screen.

Table 165 Advanced Application > Private VLAN

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
Mode	This is the type of VLAN mapped to this port. • **Normal**: These are ports in a static VLAN. This is not a private VLAN. • **Promiscuous**: Ports in a **Primary** VLAN are **Promiscuous**. They can communicate with all ports in the **Primary** VLAN and associated **Community** and **Isolated** VLANs. They cannot communicate with **Promiscuous** ports in different primary VLANs. • **Community**: Ports in a **Community** VLAN can communicate with **Promiscuous** ports in an associated Primary VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in an **Isolated** VLAN, non-associated **Primary** VLAN **Promiscuous** ports nor **Community** ports in different **Community** VLANs. • **Isolated:** Ports in an **Isolated** VLAN can communicate with **Promiscuous** ports in an associated **Primary** VLAN only. They cannot communicate with other **Isolated** ports in the same **Isolated** VLAN, non-associated **Primary** VLAN **Promiscuous** ports nor any **Community** ports.
Associated VLAN	Enter the VLAN ID of a previously created VLAN here. Note: The VLAN ID and **Mode** selected here must be the same as the VLAN ID and **VLAN Type** created in **Advanced Application > VLAN > Static VLAN**.
Tagged	A VLAN ID tag identifies VLAN membership of a frame across switches. Select this if the VLAN includes ports on multiple switches. The Switch forwards tagged frames through this port; it adds the PVID to untagged frames before sending them out. Clear this if the VLAN includes ports on this Switch only. The Switch forwards untagged frames through this port; it removes the VLAN ID from tagged frames before sending them out.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34

Green Ethernet

This chapter shows you how to configure the Switch to reduce the power consumed by switch ports.

34.1 Green Ethernet Overview

Green Ethernet reduces switch port power consumption in the following ways.

- IEEE 802.3az Energy Efficient Ethernet (EEE)

  If EEE is enabled, both sides of a link support EEE and there is no traffic, the port enters Low Power Idle (LPI) mode. LPI mode turns off some functions of the physical layer (becomes quiet) to save power. Periodically the port transmits a REFRESH signal to allow the link partner to keep the link alive. When there is traffic to be sent, a WAKE signal is sent to the link partner to return the link to active mode.

- Auto Power Down

  Auto Power Down turns off almost all functions of the port's physical layer functions when the link is down, so the port only uses power to check for a link up pulse from the link partner. After the link up pulse is detected, the port wakes up from **Auto Power Down** and operates normally.

- Short Reach

  Traditional Ethernet transmits all data with enough power to reach the maximum cable length. Shorter cables lose less power, so **Short Reach** saves power by adjusting the transmit power of each port according to the length of cable attached to that port.

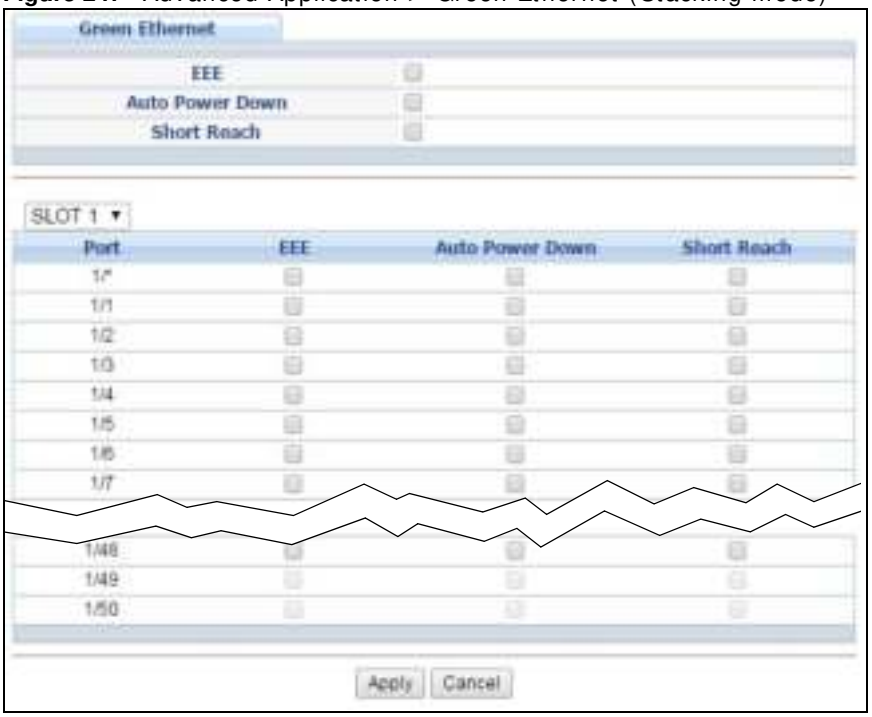
34.2 Configuring Green Ethernet

Click **Advanced Application** > **Green Ethernet** in the navigation panel to display the screen as shown.

Note: EEE, Auto Power Down and Short Reach are not supported on an uplink port.

Figure 246 Advanced Application > Green Ethernet (Standalone mode)

Figure 247 Advanced Application > Green Ethernet (Stacking mode)



The following table describes the labels in this screen.

Table 166 Advanced Application > Green Ethernet

LABEL	DESCRIPTION
EEE	Select this to activate Energy Efficient Ethernet globally.
Auto Power Down	Select this to activate Auto Power Down globally.
Short Reach	Select this to activate Short Reach globally.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
1/*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
EEE	Select this to activate Energy Efficient Ethernet on this port.
Auto Power Down	Select this to activate Auto Power Down on this port.
Short Reach	Select this to activate Short Reach on this port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35

Link Layer Discovery Protocol (LLDP)

35.1 LLDP Overview

The LLDP (Link Layer Discovery Protocol) is a layer 2 protocol. It allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps an administrator discover network changes and perform necessary network reconfiguration and management. The device information is encapsulated in the LLDPDUs (LLDP data units) in the form of TLV (Type, Length, Value). Device information carried in the received LLDPDUs is stored in the standard MIB.

The Switch supports these basic management TLVs.

- End of LLDPDU (mandatory)
- Chassis ID (mandatory)
- Port ID (mandatory)
- Time to Live (mandatory)
- Port Description (optional)
- System Name (optional)
- System Description (optional)
- System Capabilities (optional)
- Management Address (optional)

The Switch also supports the IEEE 802.1 and IEEE 802.3 organizationally-specific TLVs.

IEEE 802.1 specific TLVs:

- Port VLAN ID TLV (optional)
- Port and Protocol VLAN ID TLV (optional)

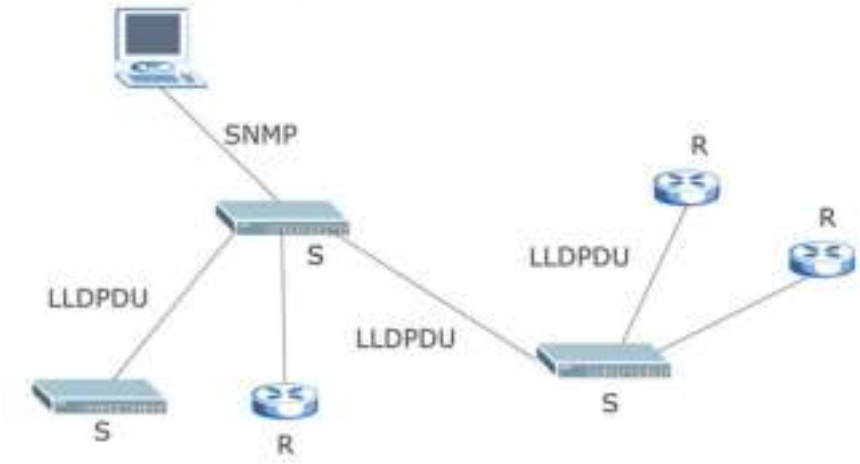
IEEE 802.3 specific TLVs:

- MAC/PHY Configuration/Status TLV (optional)
- Power via MDI TLV (optional, For PoE models only)
- Link Aggregation TLV (optional)
- Maximum Frame Size TLV (optional)

The optional TLVs are inserted between the Time To Live TLV and the End of LLDPDU TLV.

The next figure demonstrates that the network devices Switches and Routers (S and R) transmit and receive device information via LLDPDU and the network manager can query the information using Simple Network Management Protocol (SNMP).

Figure 248 LLDP Overview



35.2 LLDP-MED Overview

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension to the standard LLDP developed by the Telecommunications Industry Association (TIA) TR-41.4 subcommittee which defines the enhanced discovery capabilities, such as VoIP applications, to enable network administrators manage their network topology application more efficiently. Unlike the traditional LLDP, which has some limitations when handling multiple application devices, the LLDP-MED offers display of accurate physical topology, interoperability of devices, and easy trouble shooting for misconfigured IP addresses. There are three classes of endpoint devices that the LLDP-MED supports:

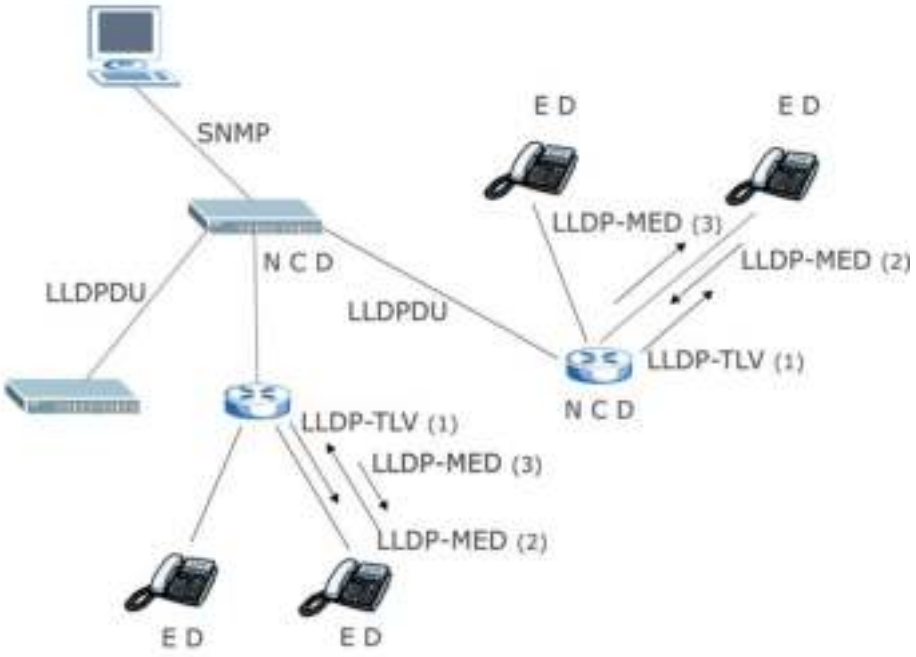
Class I: IP Communications Controllers or other communication related servers

Class II: Voice Gateways, Conference Bridges or Media Servers

Class III: IP-Phones, PC-based Softphones, End user Communication Appliances supporting IP Media

The following figure shows that with the LLDP-MED, network connectivity devices (NCD) like Switches and Routers will transmit LLDP TLV to endpoint device (ED) like IP Phone first (1), to get its device type and capabilities information, then it will receive that information in LLDP-MED TLV back from endpoint devices (2), after that the network connectivity devices will transmit LLDP-MED TLV (3) to provision the endpoint device to such that the endpoint device's network policy and location identification information is updated. Since LLDPDU updates status and configuration information periodically, network managers may check the result of provision via remote status. The remote status is updated by receiving LLDP-MED TLVs from endpoint devices.

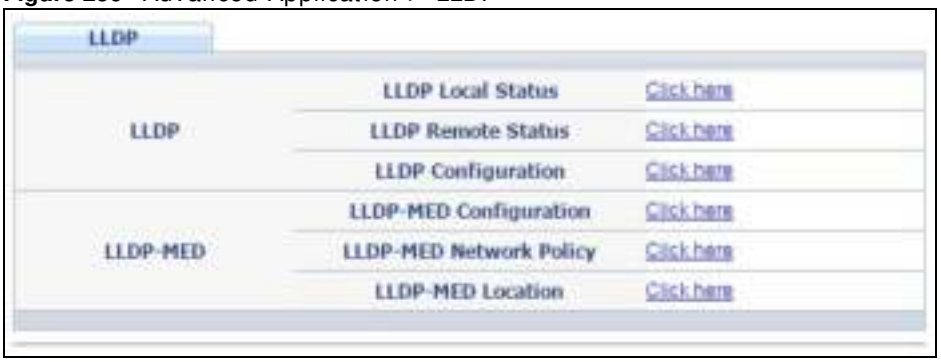
Figure 249 LLDP-MED Overview



35.3 LLDP Screens

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

Figure 250 Advanced Application > LLDP



The following table describes the labels in this screen.

Table 167 Advanced Application > LLDP

LABEL	DESCRIPTION
LLDP	
LLDP Local Status	Click here to show a screen with the Switch's LLDP information.
LLDP Remote Status	Click here to show a screen with LLDP information from the neighboring devices.
LLDP Configuration	Click here to show a screen to configure LLDP parameters.

Table 167 Advanced Application > LLDP (continued)

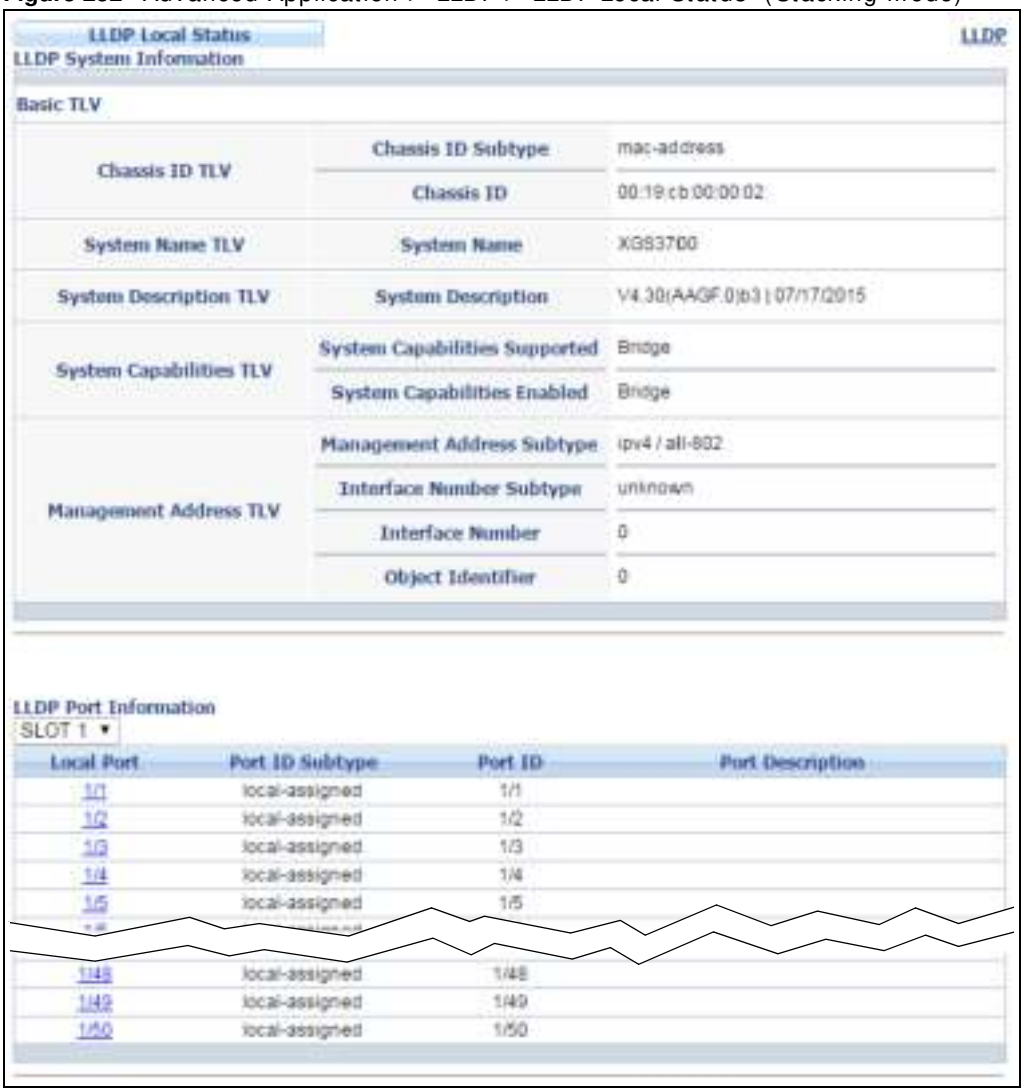
LABEL	DESCRIPTION
LLDP-MED	
LLDP-MED Configuration	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) parameters.
LLDP-MED Network Policy	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) network policy parameters.
LLDP-MED Location	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) location parameters.

35.4 LLDP Local Status

This screen displays a summary of LLDP status on this Switch. Click **Advanced Application** > **LLDP** > **LLDP Local Status** to display the screen as shown next.

Figure 251 Advanced Application > LLDP > LLDP Local Status (Standalone mode)

Figure 252 Advanced Application > LLDP > LLDP Local Status (Stacking mode)



The following table describes the labels in this screen.

Table 168 Advanced Application > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	This displays the chassis ID of the local Switch, that is the Switch you're configuring. The chassis ID is identified by the chassis ID subtype. Chassis ID Subtype - this displays how the chassis of the Switch is identified. Chassis ID - This displays the chassis ID of the local Switch.
System Name TLV	This shows the Host Name of the Switch.
System Description TLV	This shows the firmware version of the Switch.
System Capabilities TLV	This shows the System Capabilities enabled and supported on the local Switch. • System Capabilities Supported - Bridge • System Capabilities Enabled - Bridge

Table 168 Advanced Application > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Management Address TLV	The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher layer entities to assist discovery by network management. The TLV may also include the system interface number and an object identifier (OID) that are associated with this management address. This field displays the Management Address settings on the specified port(s). • Management Address Subtype - ipv4 / all-802 • Interface Number Subtype - unknown • Interface Number - 0 (not supported) • Object Identifier - 0 (not supported)
LLDP Port Information	This displays the local port information.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Local Port	This displays the number of the Switch port which receives the LLDPDU from the remote device. Click a port number to view the detailed LLDP status on this port at **LLDP Local Port Status Detail** screen. For Stacking mode, the first field box is the Slot ID, the second field box is the port.
Port ID Subtype	This indicates how the port ID field is identified.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted.
Port Description	This shows the port description that the Switch will advertise from this port.

35.4.1 LLDP Local Port Status Detail

This screen displays detailed LLDP status for each port on this Switch. Click **Advanced Application > LLDP > LLDP Local Status** and then click a port number, for example 1 in the **Local Port** column to display the screen as shown next.

Figure 253 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (Basic TLV)

LLDP Local Port Status Detail — LLDP Local Status

Local Port: 1

Basic TLV		
Port ID TLV	Port ID Subtype	local-assigned
	Port ID	1
Port Description TLV	Port Description	
Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	1
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	Yes
	AN Enabled	Yes
	AN Advertised Capability	10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD
	Oper MAU Type	30
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	No
	Aggregated Port ID	1
Max Frame Size TLV	Max Frame Size	1518

Figure 254 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (MED TLV)

The following table describes the labels in this screen.

Table 169 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LABEL	DESCRIPTION
Basic TLV	These are the Basic TLV flags
Port ID TLV	The port ID TLV identifies the specific port that transmitted the LLDP frame. • Port ID Subtype: This shows how the port is identified. • Port ID: This is the ID of the port. In stacking mode, the first number represents the slot and the second the port number.
Port Description TLV	This displays the local port description.
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID sent by the IEEE 802.1 Port VLAN ID TLV.

Table 169 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LABEL	DESCRIPTION
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLVs, which indicates whether the VLAN is enabled and supported.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. • AN Supported - Displays if the port supports or does not support auto-negotiation. • AN Enabled - The current auto-negotiation status of the port. • AN Advertised Capability - The auto-negotiation capabilities of the port. • Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port.
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. • Aggregation Capability — The current aggregation capability of the port. • Aggregation Status — The current aggregation status of the port. • Aggregation Port ID — The aggregation ID of the current port.
Max Frame Size TLV	This displays the maximum supported frame size in octets.
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This field displays which LLDP-MED TLV are capable to transmit on the Switch. • Network Policy • Location • Extend Power via MDI PSE • Extend Power via MDI PD • Inventory Management
Device Type TLV	This is the LLDP-MED device class. The ZyXEL Switch device type is: • Network Connectivity
Network Policy TLV	This displays a network policy for the specified application. • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling
Location Identification TLV	This shows the location information of a caller by its ELIN (Emergency Location Identifier Number) or the IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). • Coordinate-base LCI - latitude, longitude and altitude coordinates of the location Configuration Information (LCI) • Civic LCI - IETF Geopriv Civic Address based Location Configuration Information • ELIN - (Emergency Location Identifier Number)

35.5 LLDP Remote Status

This screen displays a summary of LLDP status for each LLDP connection to a neighboring Switch. Click **Advanced Application** > **LLDP** > **LLDP Remote Status** to display the screen as shown next.

Figure 255 Advanced Application > LLDP > LLDP Remote Status (Standalone mode)

Figure 256 Advanced Application > LLDP > LLDP Remote Status (Stacking mode)

The following table describes the labels in this screen.

Table 170 Advanced Application > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Index	The index number shows the number of remote devices that are connected to the Switch. Click on an index number to view the detailed LLDP status for this remote device in the **LLDP Remote Port Status Detail** screen.
Local Port	This is the number of the Switch's port that received LLDPDU from the remote device. In stacking mode, the first number represents the slot and the second the port number.
Chassis ID	This displays the chassis ID of the remote device associated with the transmitting LLDP agent. The chassis ID is identified by the chassis ID subtype. For example, the MAC address of the remote device.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted. The port ID is identified by the port ID subtype.
Port Description	This displays a description for the port from which this LLDPDU was transmitted.
System Name	This displays the system name of the remote device.
Management Address	This displays the management address of the remote device. It could be the MAC address or IP address. You can click on the IP address hyperlink directly.

35.5.1 LLDP Remote Port Status Detail

This screen displays detailed LLDP status of the remote device conencted to the Switch. Click **Advanced Application** > **LLDP** > **LLDP Remote Status** and then click an index number, for example 1, in the **Index** column in the **LLDP Remote Status** screen to display the screen as shown next.

Figure 257 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

The following table describes the labels in Basic TLV part of the screen.

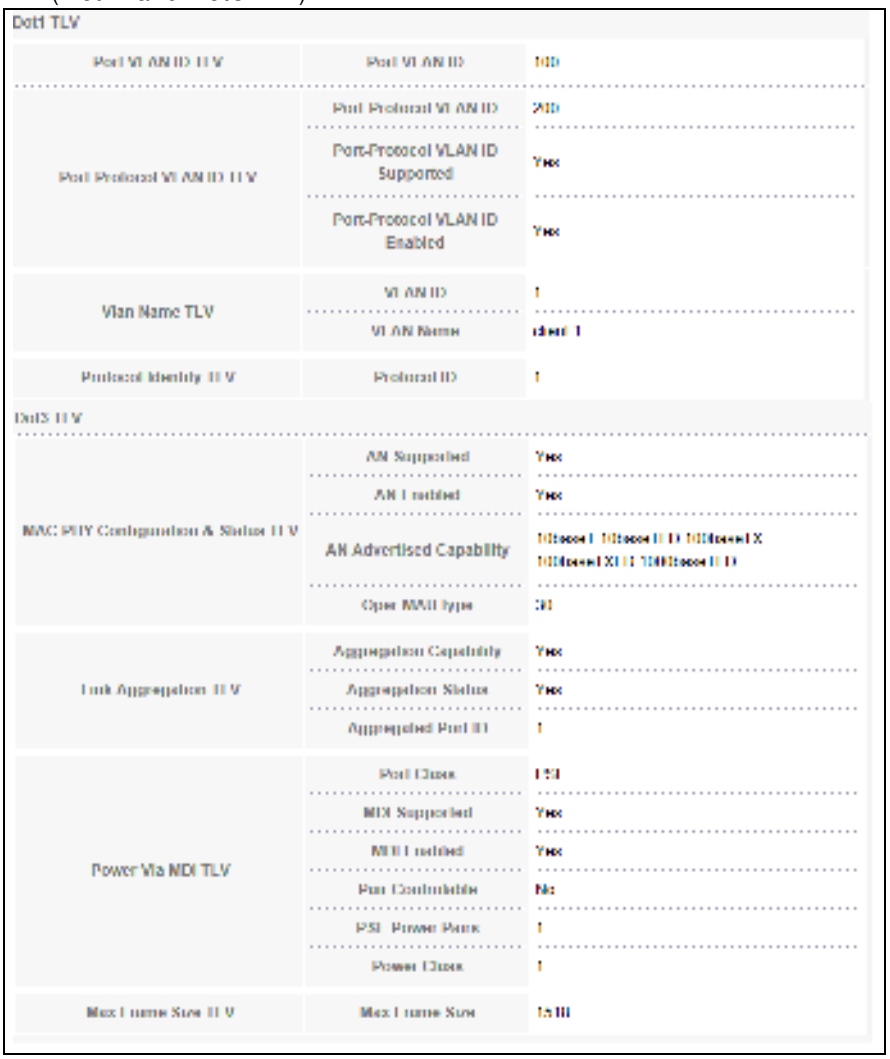
Table 171 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LABEL	DESCRIPTION
Local Port	This displays the number of the Switch's port to which the remote device is connected.
Basic TLV	
Chassis ID TLV	• Chassis ID Subtype - this displays how the chassis of the remote device is identified. • Chassis ID - this displays the chassis ID of the remote device. The chassis ID is identified by the chassis ID subtype
Port ID TLV	• Port ID Subtype - this displays how the port of the remote device is identified. • Port ID - this displays the port ID of the remote device. The port ID is identified by the port ID subtype.
Time To Live TLV	This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP frames transmitting interval.
Port Description TLV	This displays the remote port description.

Table 171 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LABEL	DESCRIPTION
System Name TLV	This displays the system name of the remote device.
System Description TLV	This displays the system description of the remote device.
System Capabilities TLV	This displays whether the system capabilities are enabled and supported on the remote device. • System Capabilities Supported • System Capabilities Enabled
Management Address TLV	This displays the following management address parameters of the remote device. • Management Address Subtype • Management Address • Interface Number Subtype • Interface Number • Object Identifier

Figure 258 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail> (Dot 1 and Dot3 TLV)

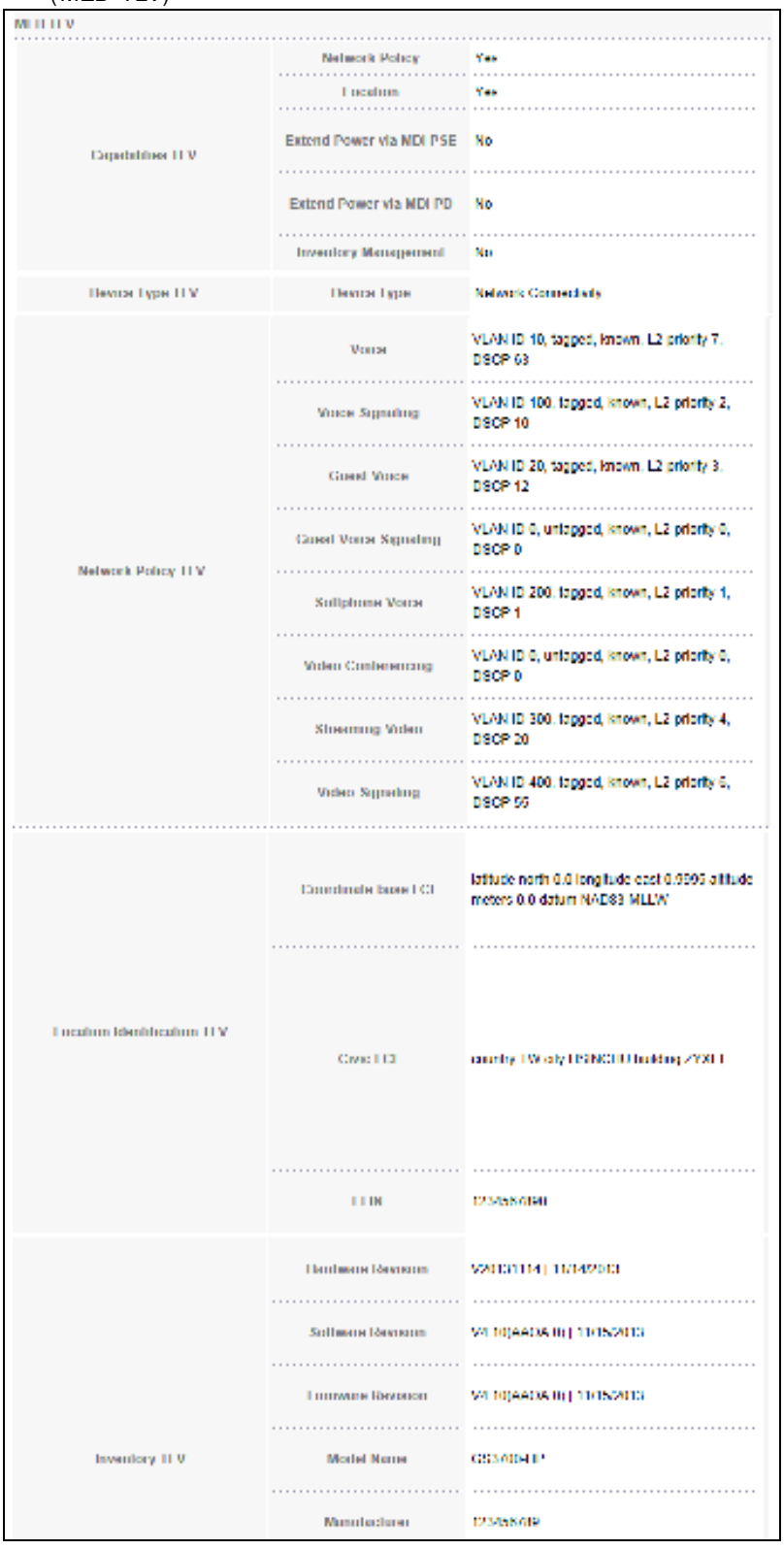


The following table describes the labels in the Dot1 and Dot3 parts of the screen.

Table 172 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID of this port on the remote device.
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLV, which indicates whether the VLAN ID and whether it is enabled and supported on the port of remote Switch which sent the LLDPDU. • Port-Protocol VLAN ID • Port-Protocol VLAN ID Supported • Port-Protocol VLAN ID Enabled
Vlan Name TLV	This shows the VLAN ID and name for remote device port. • VLAN ID • VLAN Name
Protocol Identity TLV	The Protocol Identity TLV allows the Switch to advertise the particular protocols that are accessible through its port.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. • AN Supported - Displays if the port supports or does not support auto-negotiation. • AN Enabled - The current auto-negotiation status of the port. • AN Advertised Capability - The auto-negotiation capabilities of the port. • Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. • Aggregation Capability — The current aggregation capability of the port. • Aggregation Status — The current aggregation status of the port. • Aggregation Port ID — The aggregation ID of the current port.
Power Via MDI TLV	The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controlable • PSE Power Pairs • Power Class
Max Frame Size TLV	This displays the maximum supported frame size in octets.

Figure 259 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)



The following table describes the labels in the MED TLV part of the screen.

Table 173 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

LABEL	DESCRIPTION
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This displays the MED capabilities the remote port supports. • Network Policy • Location • Extend Power via MDI PSE • Extend Power via MDI PD • Inventory Management
Device Type TLV	LLDP-MED endpoint device classes: • Endpoint Class I • Endpoint Class II • Endpoint Class III • Network Connectivity
Network Policy TLV	This displays a network policy for the specified application. • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling
Location Identification TLV	This shows the location information of a caller by its: • Coordinate-base LCI - latitude and longitude coordinates of the Location Configuration Information (LCI) • Civic LCI - IETF Geopriv Civic Address based Location Configuration Information • ELIN - (Emergency Location Identifier Number)

Table 173 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV) (continued)

LABEL	DESCRIPTION
Inventory TLV	The majority of IP Phones lack support of management protocols such as SNMP, so LLDP-MED inventory TLVs are used to provide their inventory information to the Network Connectivity Devices such as the Switch. The Inventory TLV may contain the following information. • Hardware Revision • Software Revision • Firmware Revision • Model Name • Manufacturer • Serial Number • Asset ID
Extended Power via MDI TLV	Extended Power Via MDI Discovery enables detailed power information to be advertised by Media Endpoints, such as IP phones and Network Connectivity Devices such as the Switch. • Power Type - whether it is currently operating from primary power or is on backup power (backup power may indicate to the Endpoint Device that it should move to a power conservation mode). • Power Source - whether or not the Endpoint is currently operating from an external power source. • Power Priority - the Endpoint Device's power priority (which the Network Connectivity Device may use to prioritize which devices will remain in service during power shortages) • Power Value - power requirement, in fractions of Watts, in current configuration

35.6 LLDP Configuration

Use this screen to configure global LLDP settings on the Switch. Click **Advanced Application** > **LLDP > LLDP Configuration** to display the screen as shown next.

Figure 260 Advanced Application > LLDP > LLDP Configuration (Standalone mode)

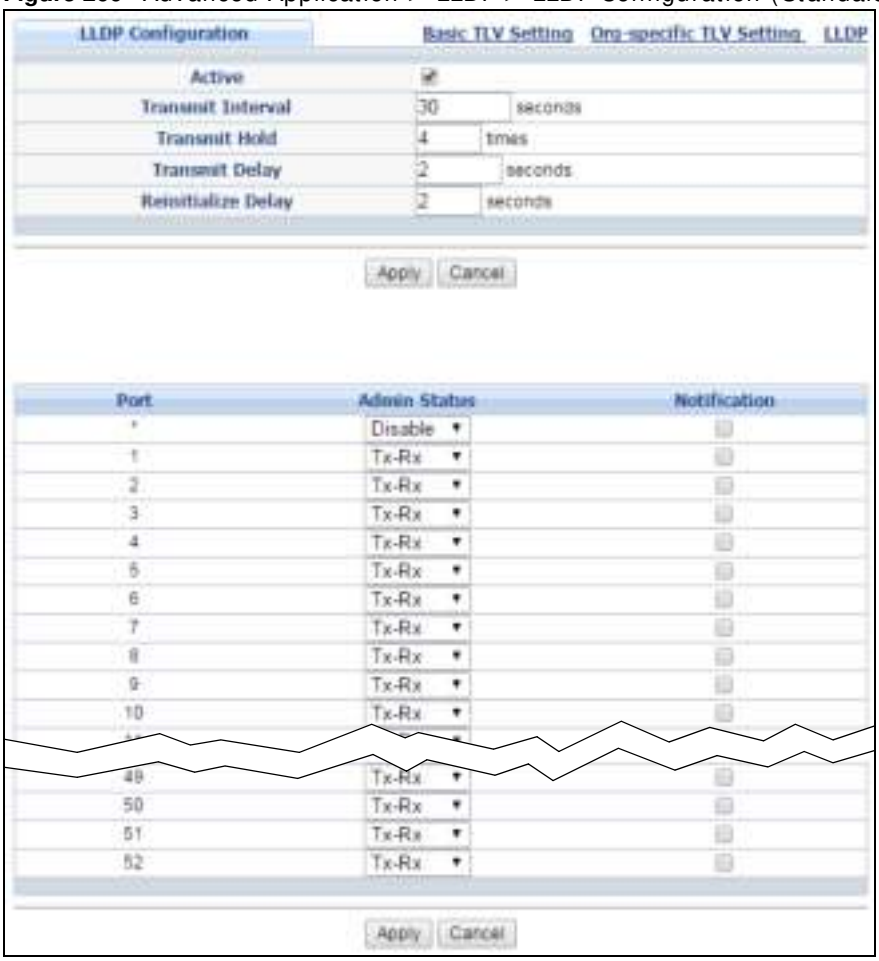
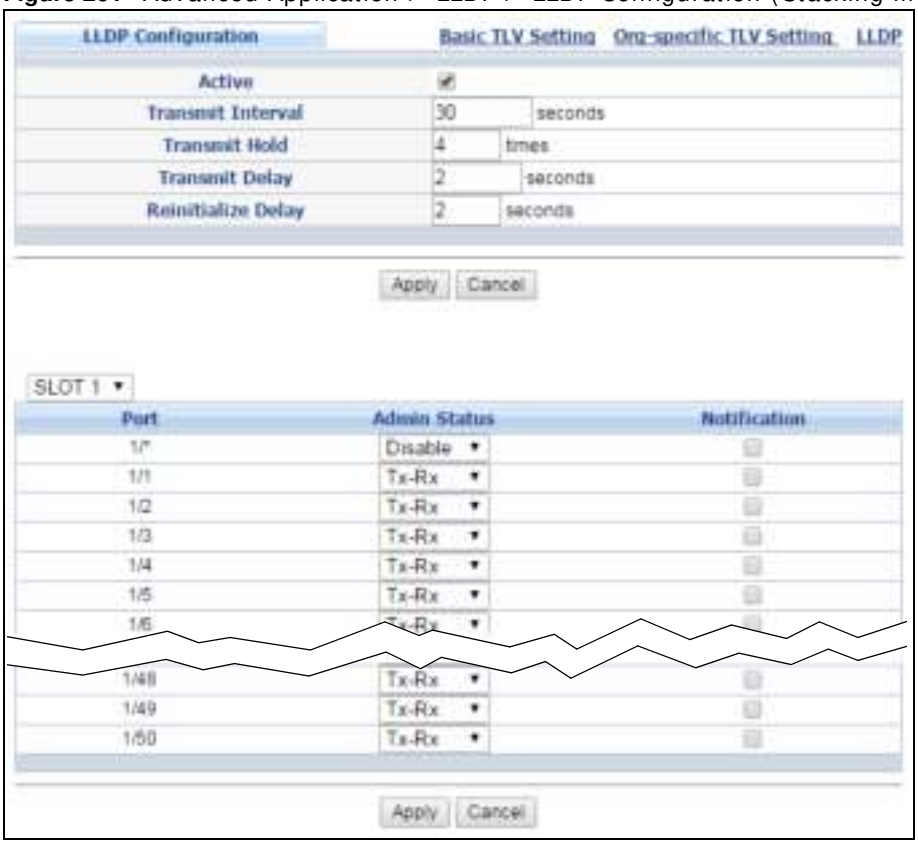


Figure 261 Advanced Application > LLDP > LLDP Configuration (Stacking mode)



The following table describes the labels in this screen.

Table 174 Advanced Application > LLDP > LLDP Configuration

LABEL	DESCRIPTION
Active	Select to enable LLDP on the Switch. It is enabled by default.
Transmit Interval	Enter how many seconds the Switch waits before sending LLDP packets.
Transmit Hold	Enter the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP packets transmitting interval.
Transmit Delay	Enter the delay (in seconds) between successive LLDPDU transmissions initiated by value or status changes in the Switch MIB.
Reinitialize Delay	Enter the number of seconds for LLDP to wait before initializing on a port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the Switch's port number. * means all ports (on the same Switch). In Stacking mode, the first number means Slot ID and the second is the port.

Table 174 Advanced Application > LLDP > LLDP Configuration

LABEL	DESCRIPTION
Admin Status	Select whether LLDP transmission and/or reception is allowed on this port. • Disable - not allowed • Tx-Only - transmit only • Rx-Only - receive only • Tx-Rx - transmit and receive
Notification	Select whether LLDP notification is enabled on this port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.6.1 LLDP Configuration Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **Advanced Application** > **LLDP** > **LLDP Configuration** > **Basic TLV Setting** to display the screen as shown next.

Figure 262 Advanced Application > LLDP > LLDP Configuration> Basic TLV Setting (Standalone mode)

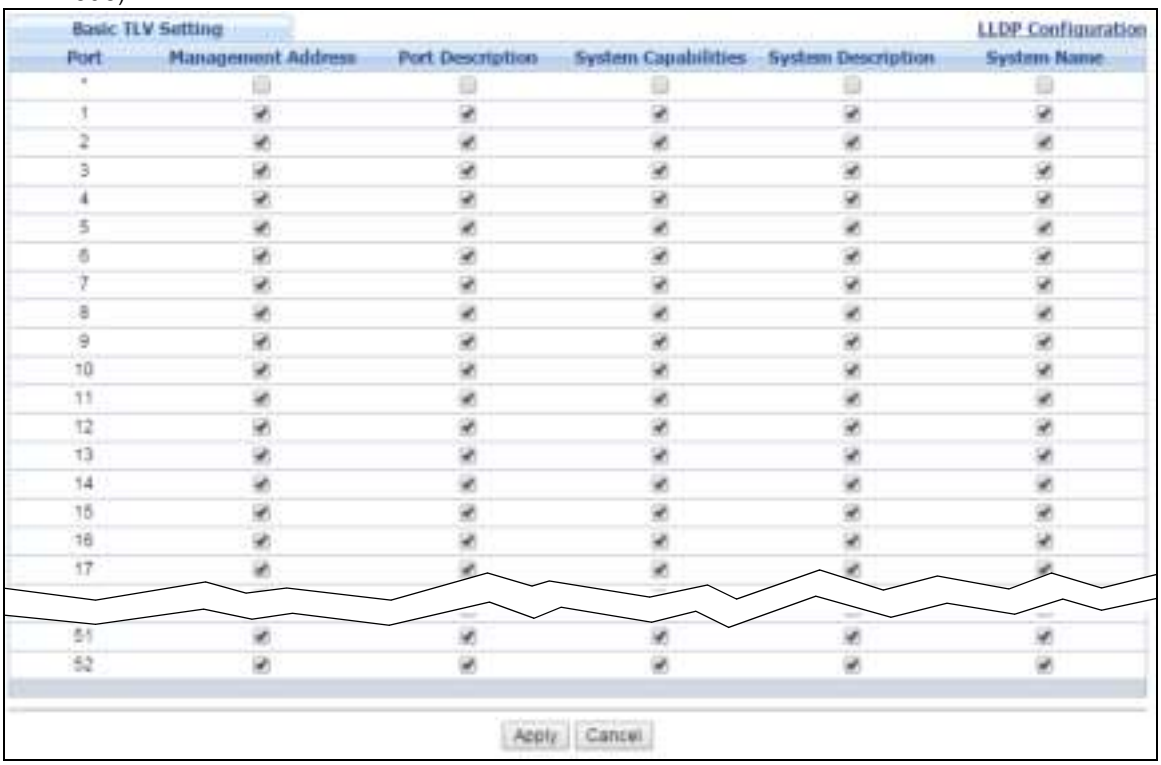
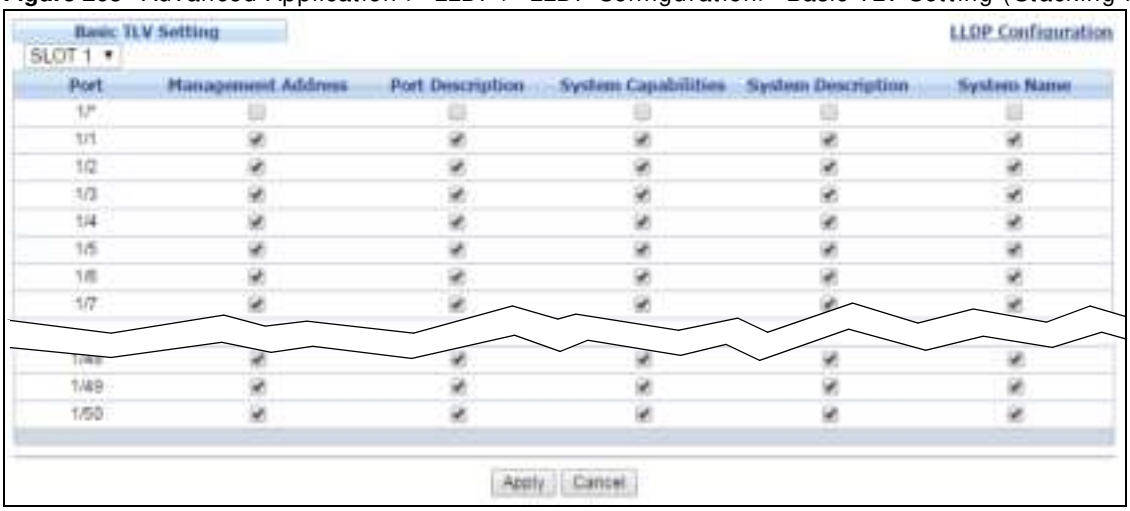


Figure 263 Advanced Application > LLDP > LLDP Configuration> Basic TLV Setting (Stacking mode)



The following table describes the labels in this screen.

Table 175 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the Switch's port number.
Management Address	Select the check box(es) to enable or disable the sending of Management Address TLVs on the port(s).
Port Description	Select the check box(es) to enable or disable the sending of Port Description TLVs on the port(s).
System Capabilities	Select the check box(es) to enable or disable the sending of System Capabilities TLVs on the port(s).
System Description	Select the check box(es) to enable or disable the sending of System Description TLVs on the port(s).
System Name	Select the check box(es) to enable or disable the sending of System Name TLVs on the port(s).
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.6.2 LLDP Configuration Basic Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **Advanced Application** > **LLDP > LLDP Configuration > Org-specific TLV Setting** to display the screen as shown next.

Figure 264 Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting (Standalone mode)

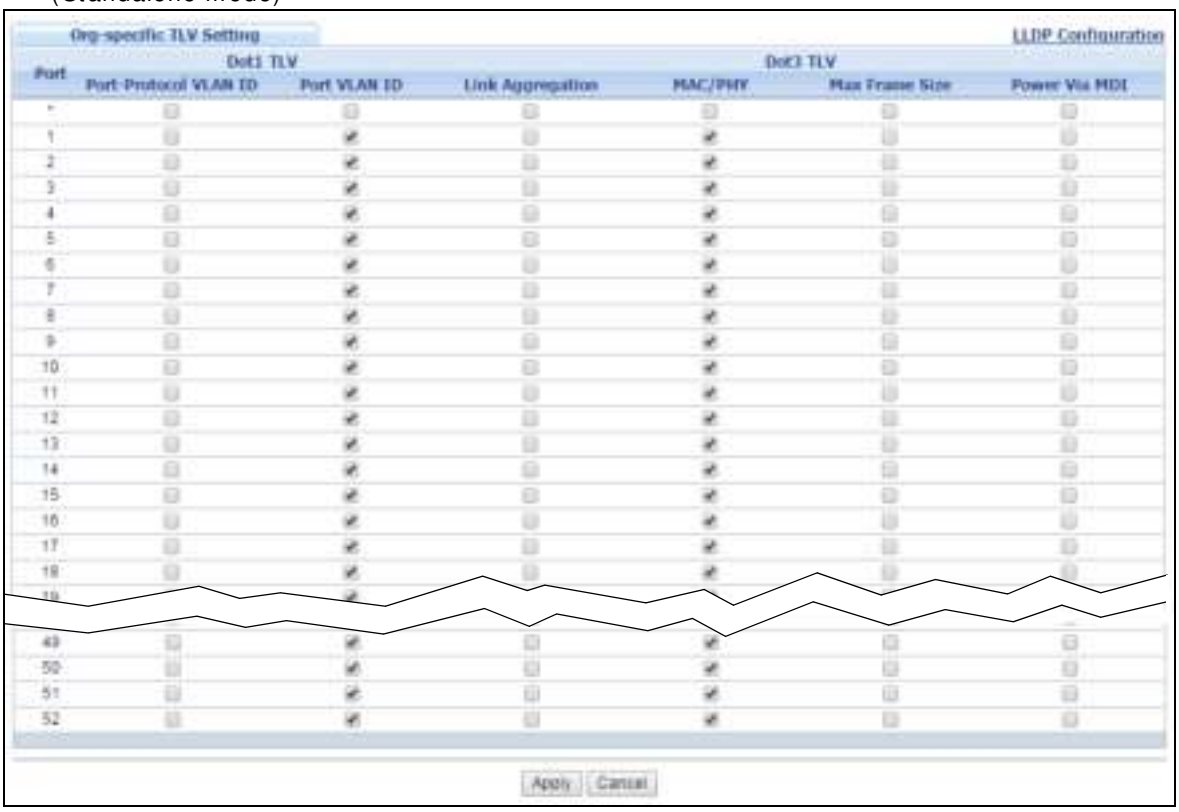
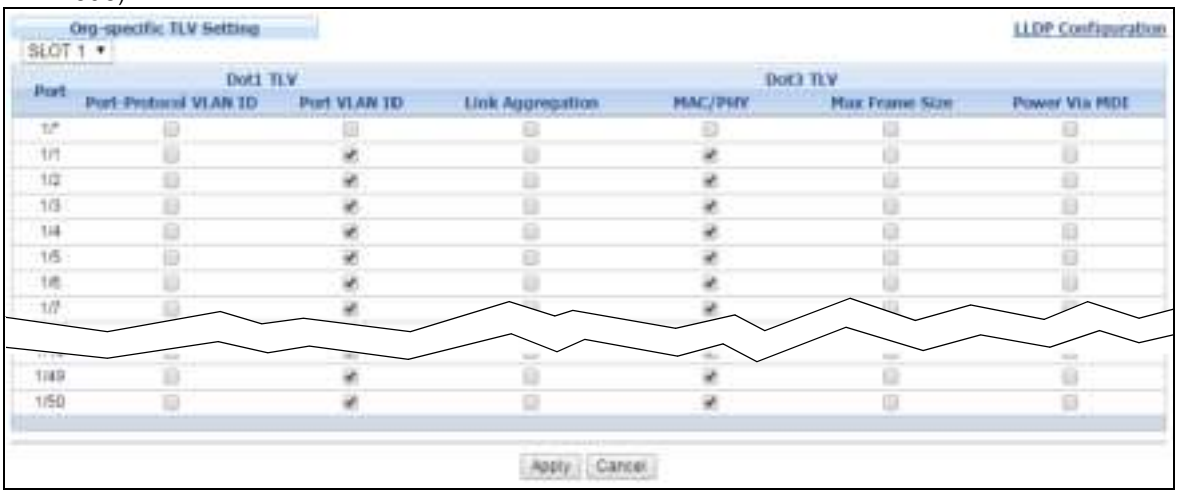


Figure 265 Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting (Stacking mode)



The following table describes the labels in this screen.

Table 176 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the Switch's port number.
Dot1 TLV	

Table 176 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

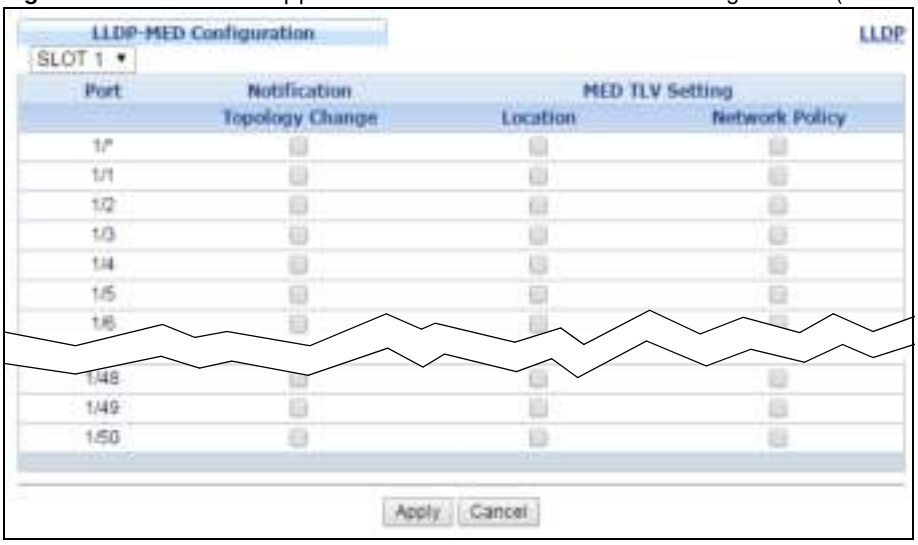
LABEL	DESCRIPTION
Port-Protocol VLAN ID	Select the check box(es) to enable or disable the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs on the port(s).
Port VLAN ID	Select the check box(es) to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the port(s). All check boxes in this column are enabled by default.
Dot3 TLV	
Link Aggregation	Select the check box(es) to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the port(s).
MAC/PHY	Select the check box(es) to enable or disable the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the port(s). All check boxes in this column are enabled by default.
Max Frame Size	Select the check box(es) to enable or disable the sending of IEEE 802.3 Max Frame Size TLVs on the port(s).
Power Via MDI	Note: For PoE models only. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controlable • PSE Power Pairs • Power Class
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.7 LLDP-MED Configuration

Click **Advanced Application** > **LLDP** > **LLDP-MED Configuration** to display the screen as shown next.

Figure 266 Advanced Application > LLDP > LLDP-MED Configuration (Standalone mode)

Figure 267 Advanced Application > LLDP > LLDP-MED Configuration (Stacking mode)



The following table describes the labels in this screen.

Table 177 Advanced Application > LLDP > LLDP-MED Configuration

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the Switch's port number. Select * to configure all ports (in the same Switch) simultaneously. In Stacking mode, the first number means Slot ID and the second is the port.
Notification	
Topology Change	Select to enable LLDP-MED topology change traps on this port.
MED TLV Setting	
Location	Select to enable transmitting LLDP-MED location TLV.
Network Policy	Select to enable transmitting LLDP-MED Network Policy TLV.
Apply	Click **Apply** to save the changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.8 LLDP-MED Network Policy

Click **Advanced Application** > **LLDP** > **LLDP-MED Network Policy** to display the screen as shown next.

Figure 268 Advanced Application > LLDP > LLDP-MED Network Policy (Standalone mode)

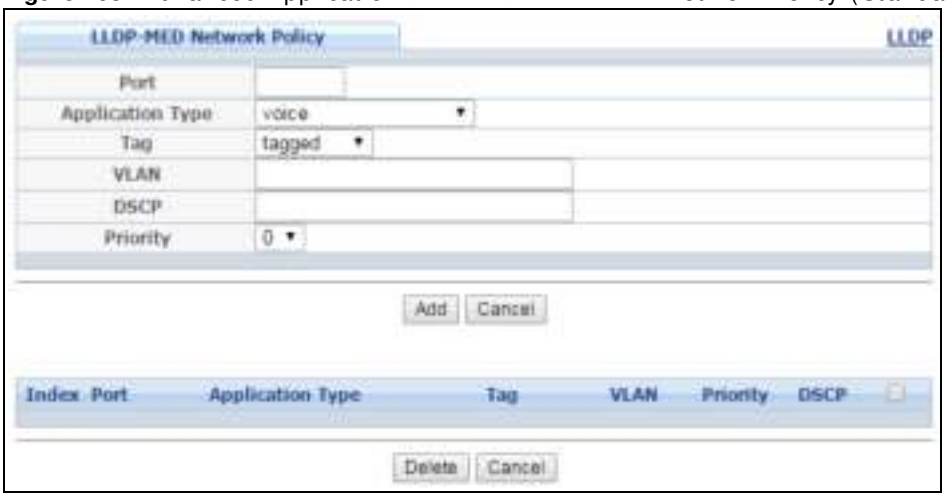
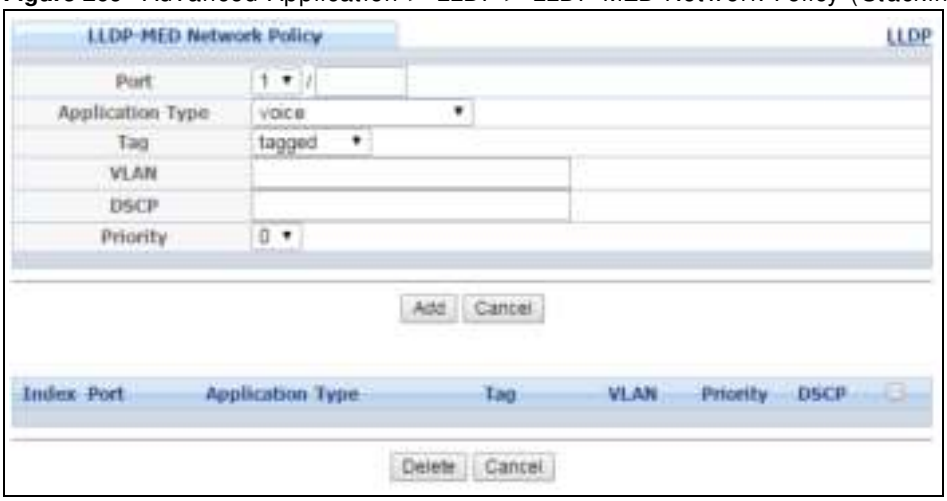


Figure 269 Advanced Application > LLDP > LLDP-MED Network Policy (Stacking mode)



The following table describes the labels in this screen.

Table 178 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
Port	Enter the port number to set up the LLDP-MED network policy. For Stacking mode the first field box is the Slot ID, the second field box is the port.
Application Type	Select the type of application used in the network policy. • voice • voice-signaling • guest-voice • guest-voice-signaling • softphone-voice • video-conferencing • streaming-video • video-signaling
Tag	Select to tag or untag in the network policy. • tagged • untagged
VLAN	Enter the VLAN ID number. It should be from 1 to 4094. For priority tagged frames, enter "0".
DSCP	Enter the DSCP value of the network policy. The value is defined from 0 through 63 with the 0 representing use of the default DSCP value.
Priority	Enter the priority value for the network policy.
Add	Click **Add** after finish entering the network policy information. A summary table will list all the Switch you've added.
Cancel	Click **Cancel** to begin entering the information afresh.
Index	This field displays the of index number of the network policy. Click an index number to edit the rule.
Port	This field displays the port number of the network policy. In stacking mode, the first number represents the slot and the second the port number.
Application Type	This field displays the application type of the network policy.
Tag	This field displays the Tag Status of the network policy.
VLAN	This field displays the VLANID of the network policy.
Priority	This field displays the priority value of the network policy.

Table 178 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
DSCP	This field displays the DSCP value of the network policy.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rules that you want to remove, then click the Delete button.
Cancel	Click **Cancel** to clear the selected checkboxes.

35.9 LLDP-MED Location

Click **Advanced Application** > **LLDP** > **LLDP-MED Location** to display the screen as shown next.

Figure 270 Advanced Application > LLDP > LLDP-MED Location (Standalone mode)

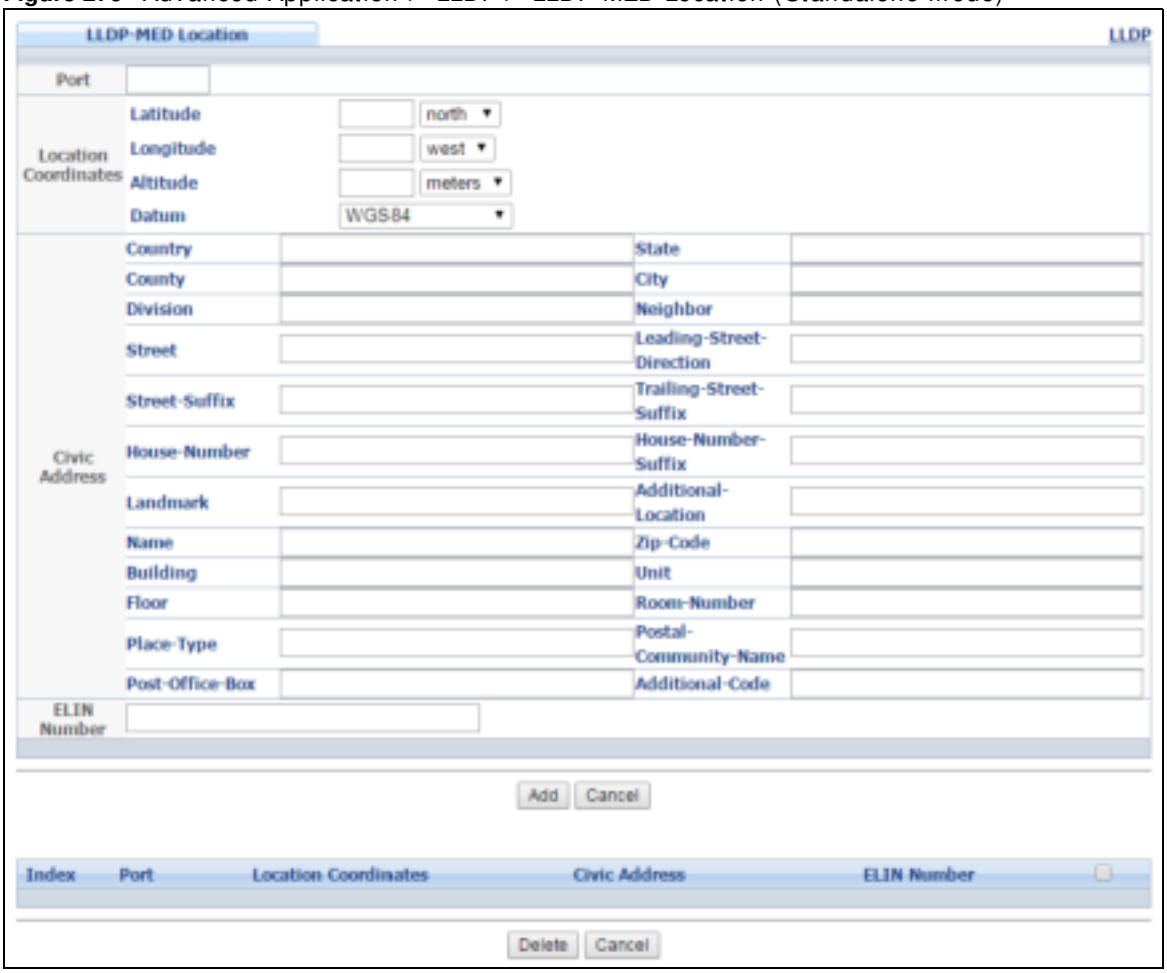
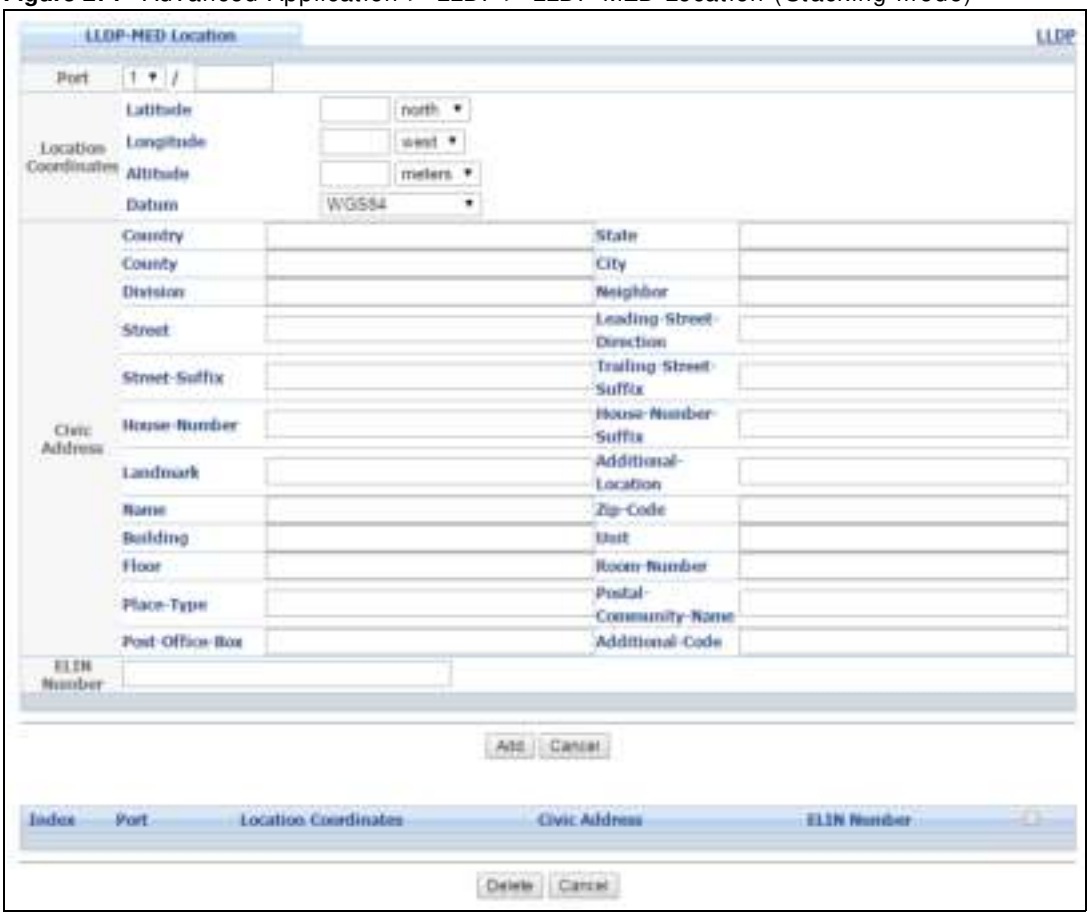


Figure 271 Advanced Application > LLDP > LLDP-MED Location (Stacking mode)



The following table describes the labels in this screen.

Table 179 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Port	Enter the port number you want to set up the location within the LLDP-MED network.For Stacking mode the first field box is the Slot ID, the second field box is the port.
Location Coordinates	The LLDP-MED uses geographical coordinates and Civic Address to set the location information of the remote device. Geographical based coordinates includes latitude, longitude, altitude and datum. Civic Address includes Country, State, County, City, Street and other related information.
Latitude	Enter the latitude information. The value should be from 0º to 90º. • north • south
Longitude	Enter the longitude information. The value should be from 0º to 180º. • west • east
Altitude	Enter the altitude information. The value should be from -2097151 to 2097151 in meters or in floors. • meters • floor

Table 179 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Datum	Select the appropriate geodetic datum used by GPS. • WGS84 • NAD83-NAVD88 • NAD83-MLLW
Civic Address	Enter the Civic Address by providing information such as Country, State, County, City, Street, Number, ZIP code and other additional information. Enter at least two field in this configuration including the Country. The valid length of the Country field is 2 characters and all other fields are up to 32 characters. • Country • State • County • City • Division • Neighbor • Street • Leading-Street-Direction • Street-Suffix • Trailing-Street-Suffix • House-Number • House-Number-Suffix • Landmark • Additional-Location • Name • Zip-Code • Building • Unit • Floor • Room-Number • Place-Type • Postal-Community-Name • Post-Office-Box • Additional-Code
ELIN Number	Enter a numerical digit string, corresponding to the ELIN identifier which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The valid length is from 10 characters to 25 characters.
Add	Click **Add** after finish entering the location information.
Cancel	Click **Cancel** to begin entering the location information afresh.
Index	This lists the index number of the location configuration. Click an index number to view or edit the location.
Port	This lists the port number of the location configuration. In stacking mode, the first number represents the slot and the second the port number.
Location Coordinates	This field displays the location configuration information based on geographical coordinates that includes longitude, latitude, altitude and datum.
Civic Address	This field displays the Civic Address for the remote device using information such as Country, State, County, City, Street, Number, ZIP code and additional information.
ELIN Number	This field shows the Emergency Location Identification Number (ELIN), which is used to identify endpoint devices when they issue emergency call services. The valid length is form 10 characters to 25 characters.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.

Table 179 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Delete	Check the locations that you want to remove, then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

36

Anti-Arpscan

36.1 Anti-Arpscan Overview

Address Resolution Protocol (ARP), RFC 826, is a protocol used to convert a network-layer IP address to a link-layer MAC address. ARP scan is used to scan the network of a certain interface for alive hosts. It shows the IP address and MAC addresses of all hosts found. Hackers could use ARP scan to find targets in your network. **Anti-arpscan** is used to detect unusual ARP scan activity and block suspicious hosts or ports.

Unusual ARP scan activity is determined by port and host thresholds that you set. A port threshold is determined by the number of packets received per second on the port. If the received packet rate is over the threshold, then the port is put into an **Err-Disable** state. You can recover the normal state of the port manually if this happens and after you identify the cause of the problem.

A host threshold is determined by the number of ARP-request packets received per second. There is a global threshold rate for all hosts. If the rate of a host is over the threshold, then that host is blocked by using a MAC address filter. A blocked host is released automatically after the MAC aging time expires.

Note: A port-based threshold must be larger than the host-based threshold or the host-based threshold will not work.

36.1.1 What You Can Do

- Use the **Anti-Arpscan Status** screen (Section 36.2 on page 373) to see what ports are trusted and are forwarding traffic or are disabled.
- Use the **Anti-Arpscan Host Status** screen (Section 36.3 on page 374) to view blocked hosts and clear selected ones.
- Use the **Anti-Arpscan Trust Host** screen (Section 36.4 on page 374) to create or remove trusted hosts identified by IP address and subnet mask. **Anti-arpscan** is not performed on trusted hosts.
- Use this **Anti-Arpscan Configure** screen (Section 36.5 on page 375) to enable anti-arpscan, set port and host thresholds as well as configure ports to be trusted or untrusted.

36.1.2 What You Need to Know

- You should set an uplink port as a trusted port before enabling **Anti-arpscan** so as to prevent the port from being shutdown due to receiving too many ARP messages.
- When a port is configured as a trusted port, **Anti-arpscan** is not performed on the port. Both host and port thresholds are ignored for trusted ports. If the received ARP packet rate on a port or the received ARP-requests from a host exceed the thresholds, the trusted port will not be closed.
- If a port on the Switch is closed by **Anti-arpscan**, and you want to recover it, then do one of the following:

  - Go to **Basic Setting > Port Setup**. Clear **Active** and click **Apply**. Then select **Active** and click **Apply** again.
  - Go to **Application > Errdiable > Errdisable Recovery** and set the interval for **Anti-arpscan**. After the interval expires, the closed port(s) will become active and start receiving packets again.
  - Use the command `port no inactive`.
- Refer to the port logs to see when a port was closed.

36.2 Anti-Arpscan Status

Use this screen to see what ports are trusted and are forwarding traffic or are disabled. To open this screen, click **Advanced Application > Anti-Arpscan**.

Figure 272 Advanced Application > Anti-Arpscan Status

The following table describes the fields in the above screen.

Table 180 Advanced Application > Anti-Arpscan Status

LABEL	DESCRIPTION
Anti-Arpscan is....	This shows whether **Anti-arpscan** is enabled or disabled on the Switch.
Port	This field displays the port number of the Switch.
Trusted	This field displays whether the port is trusted or untrusted. **Anti-arpscan** is not performed on a trusted port.
State	This field displays whether the port can forward traffic normally (**Forwarding**) or is disabled (**Err-Disable**).

36.3 Anti-Arpscan Host Status

Use this screen to view blocked hosts and unblock ones connected to certain ports. To open this screen, click **Advanced Application > Anti-Arpscan > Host Status**.

Figure 273 Advanced Application > Anti-Arpscan > Host Status

The following table describes the fields in the above screen.

Table 181 Advanced Application > Anti-Arpscan > Host Status

LABEL	DESCRIPTION
Clear Filtered host:	A filtered host is a blocked IP address.
Port List	Type a port number or a series of port numbers separated by commas and spaces, and then click **Clear** to unblock all hosts connected to these ports.
Filtered host:	This table lists information on blocked hosts.
Index	This displays the index number of an IP address (a host) that has been blocked.
Host IP	This displays the IP address of the blocked host.
MAC	This displays the MAC address of the blocked host.
VLAN	This displays the VLAN ID that shows which VLAN the blocked host is in.
Port	This displays the port number to which the blocked host is connected.
State	This shows **Err-Disable** if the ARP-request rate from this host is over the threshold. Forwarding hosts are not displayed.

36.4 Anti-Arpscan Trust Host

Use this screen to create or remove trusted hosts identified by IP address and subnet mask. **Anti-arpscan** is not performed on trusted hosts. To open this screen, click **Advanced Application > Anti-Arpscan > Trust Host**.

Figure 274 Advanced Application > Anti-Arpscan > Trust Host

The following table describes the fields in the above screen.

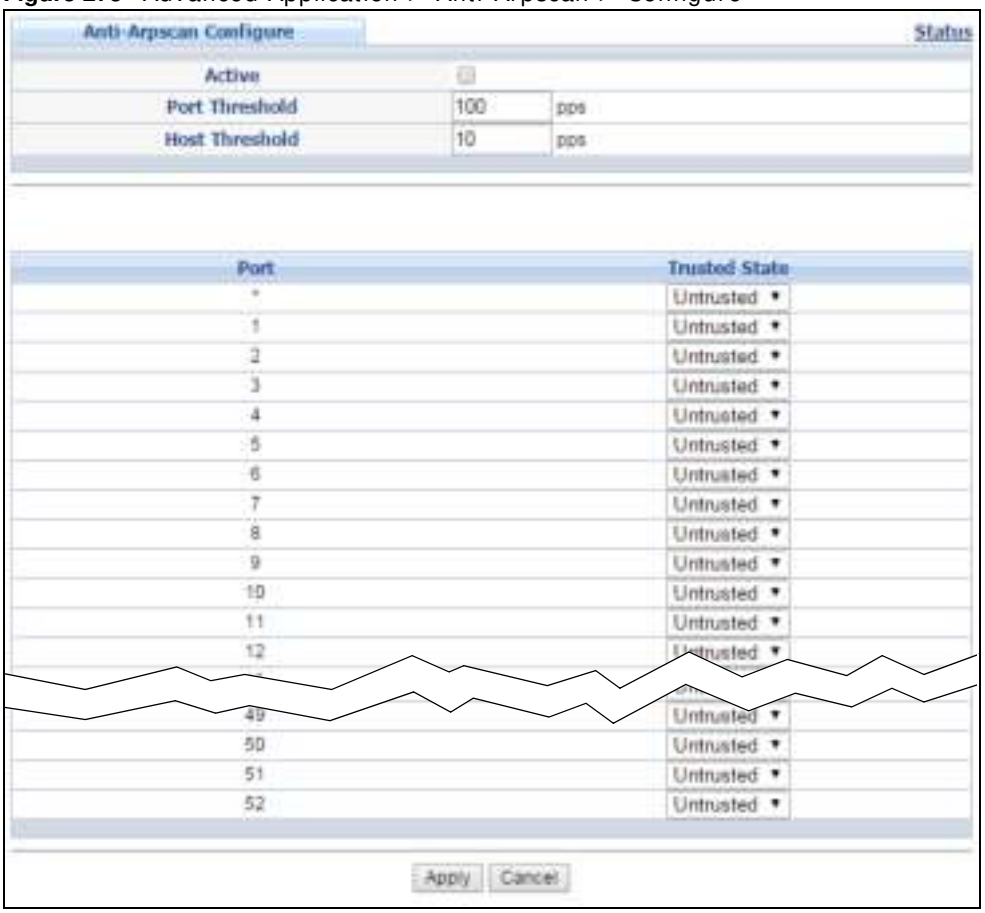
Table 182 Advanced Application > Anti-Arpscan > Trust Host

LABEL	DESCRIPTION
Name	Type a descriptive name of up to 32 printable ASCII characters to identify this host.
Host IP	Type the IP address of the host.
Mask	A trusted host may consist of a subnet of IP addresses. Type a subnet mask to create a single host or a subnet of hosts.
Add	Click this to create the trusted host.
Cancel	Click this to reset the values above based 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 trusted host.
Name	This field displays the name of the trusted host.
Host IP	This field displays the IP address of the trusted host.
Mask	This field displays the subnet mask of the trusted host.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select an entry checkbox and click **Delete** to remove the specified entry.
Cancel	Click this to clear the check boxes above.

36.5 Anti-Arpscan Configure

Use this screen to enable **Anti-Arpscan**, set port and host thresholds as well as configure ports to be trusted or untrusted. To open this screen, click **Advanced Application > Anti-Arpscan > Configure**.

Figure 275 Advanced Application > Anti-Arpscan > Configure



The following table describes the fields in the above screen.

Table 183 Advanced Application > Anti-Arpscan > Configure

LABEL	DESCRIPTION
Active	Select this to enable **Anti-arpscan** on the Switch.
Port Threshold	A port threshold is determined by the number of packets received per second on the port. If the received packet rate is over the threshold, then the port is put into an **Err-Disable** state. Type the maximum number of packets per second allowed on the port before it is blocked. Note: The allowed range is 2 to 255 packets received per second.
Host Threshold	A host threshold is determined by the number of ARP-request packets received per second. This is the global threshold rate for all hosts. If the rate of a host is over the threshold, then that host is blocked by using a MAC address filter. A blocked host is released automatically after the MAC aging time expires. Type the maximum number of ARP-request packets allowed by a host before it is blocked. Note: The allowed range is 2 to 100 ARP-request packets per second. Note: The port-based threshold must be larger than the host-based threshold or the host-based threshold will not be applied.
Port	Use port * to have all ports be **Untrusted** or **Trusted**. **Anti-arpscan** is not performed on trusted hosts.

Table 183 Advanced Application > Anti-Arpscan > Configure

LABEL	DESCRIPTION
Trusted State	Select **Untrusted** or **Trusted** for the associated port.
Apply	Click **Apply** 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 **Save** 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.

37

BPDU Guard

37.1 BPDU Guard Overview

A BPDU (Bridge Protocol Data Units) is a data frame that contains information about STP. STP-aware switches exchange BPDUs periodically.

The BPDU guard feature allows you to prevent any new STP-aware switch from connecting to an existing network and causing STP topology changes in the network. If there is any BPDU detected on the port(s) on which BPDU guard is enabled, the Switch disables the port(s) automatically. You can then enable the port(s) manually in the **Basic Setting > Port Setup** screen (Section 6.6 on page 69) or use the **Errdisable Recovery** screen (see Section 31.6 on page 331) to have the port(s) become active after a certain time interval.

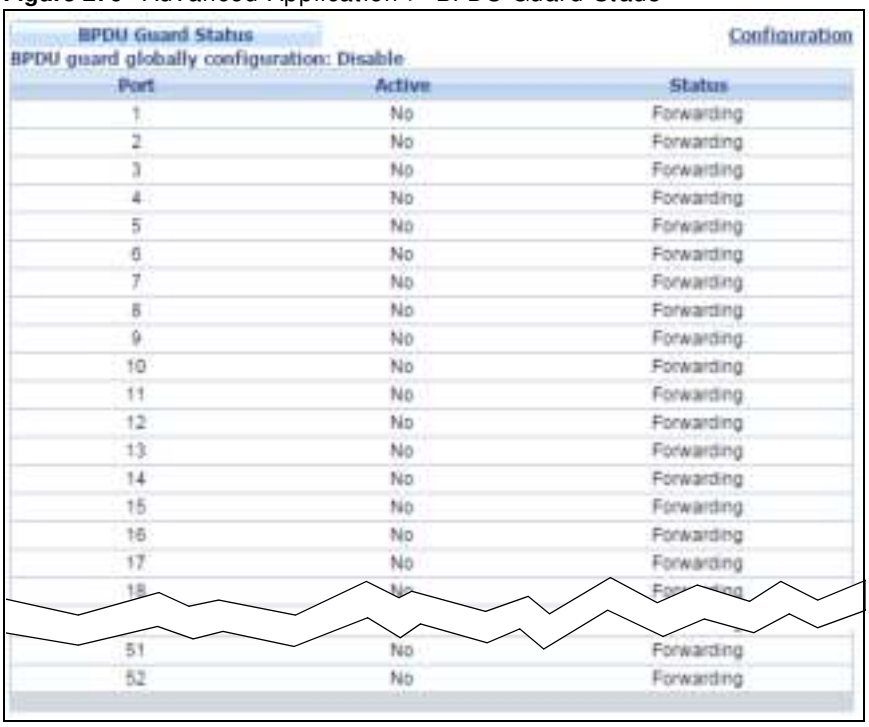
37.1.1 What You Can Do

- Use the **BPDU Guard Status** screen (Section 37.2 on page 378) to view the BPDU guard status.
- Use the **BPDU Guard Configuration** screen (Section 37.3 on page 379) to enable BPDU guard on the Switch.

37.2 BPDU Guard Status

Use this screen to view whether BPDU guard is enabled on the Switch and the port status. Click **Advanced Application** > **BPDU Guard** in the navigation panel.

Figure 276 Advanced Application > BPDU Guard Staus



The following table describes the fields in the above screen.

Table 184 Advanced Application > BPDU Guard Staus

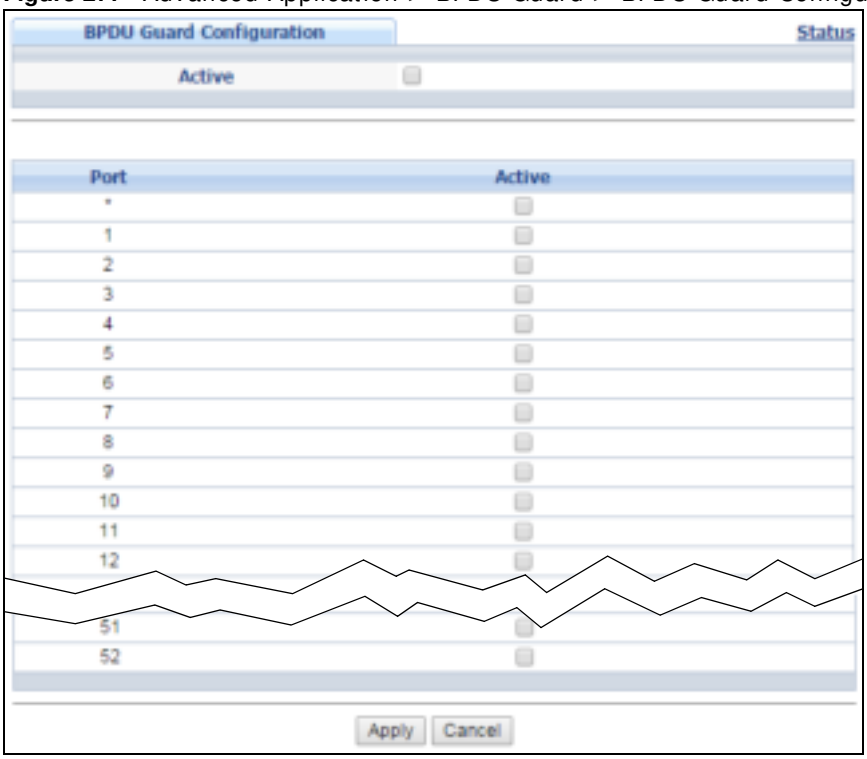
LABEL	DESCRIPTION
BPDU guard globally configuration	This field displays whether BPDU guard is activated on the Switch.
Port	This is the number of the port on the Switch.
Active	This shows whether BPDU guard is activated on the port.
Status	This shows whether the port is shut down (**Err-disable**) or able to transmit packets (**Forwarding**).

37.3 BPDU Guard Configuration

Use this screen to turn on the BPDU guard feature on the Switch and port(s).

In the **BPDU Guard Status** screen click **Configuration** to display the configuration screen as shown.

Figure 277 Advanced Application > BPDU Guard > BPDU Guard Configuration



The following table describes the fields in the above screen.

Table 185 Advanced Application > BPDU Guard > BPDU Guard Configuration

LABEL	DESCRIPTION
Active	Select this option to enable BPDU guard on the Switch.
Port	This field displays the Switch's 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.
Active	Select this check box to enable the BPDU guard feature on this port. The Switch shuts down this port if there is any BPDU received on the port. Clear this check box to disable the BPDU guard feature.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38

OAM

38.1 OAM Overview

Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units or OAM PDUs to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah. Because link layer Ethernet OAM operates at layer two of the OSI (Open Systems Interconnection Basic Reference) model, neither IP or SNMP are necessary to monitor or troubleshoot network connection problems.

The Switch supports the following IEEE 802.3ah features:

- Discovery - this identifies the devices on each end of the Ethernet link and their OAM configuration.
- Remote Loopback - this can initiate a loopback test between Ethernet devices.

38.1.1 What You Can Do

- Use the **OAM Status** screen (Section 38.2 on page 381) to view the configuration of ports on which Ethernet OAM is enabled.
- Use the **OAM Configuration** screen (Section 38.3 on page 387) to enable Ethernet OAM on the Switch.
- Use the **OAM Remote Loopback** screen (Section 38.4 on page 389) to perform remote-loopback tests.

38.2 OAM Status

Use this screen to view the configuration of ports on which Ethernet OAM is enabled. Click **Advanced Application** > **OAM** in the navigation panel.

Figure 278 Advanced Application > OAM Status (Standalone mode)

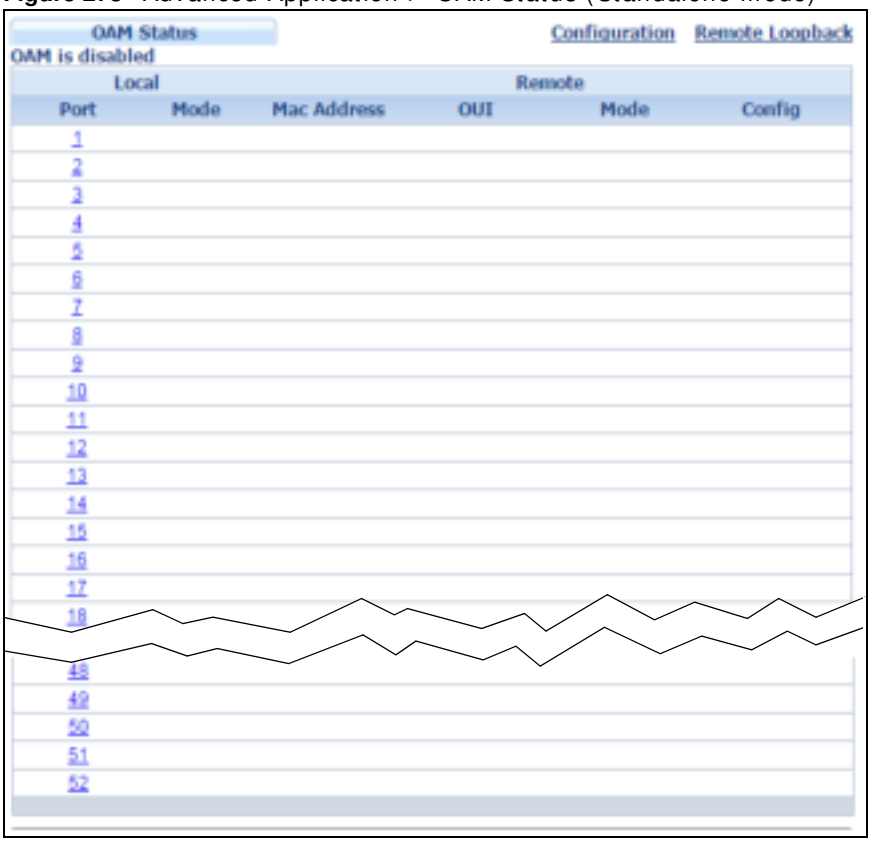
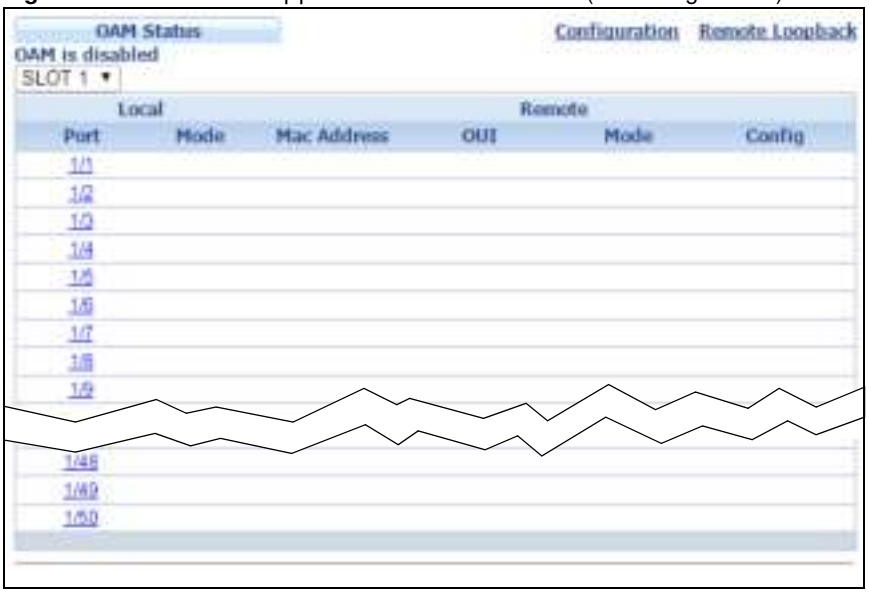


Figure 279 Advanced Application > OAM Status (Stacking mode)



The following table describes the fields in the above screen.

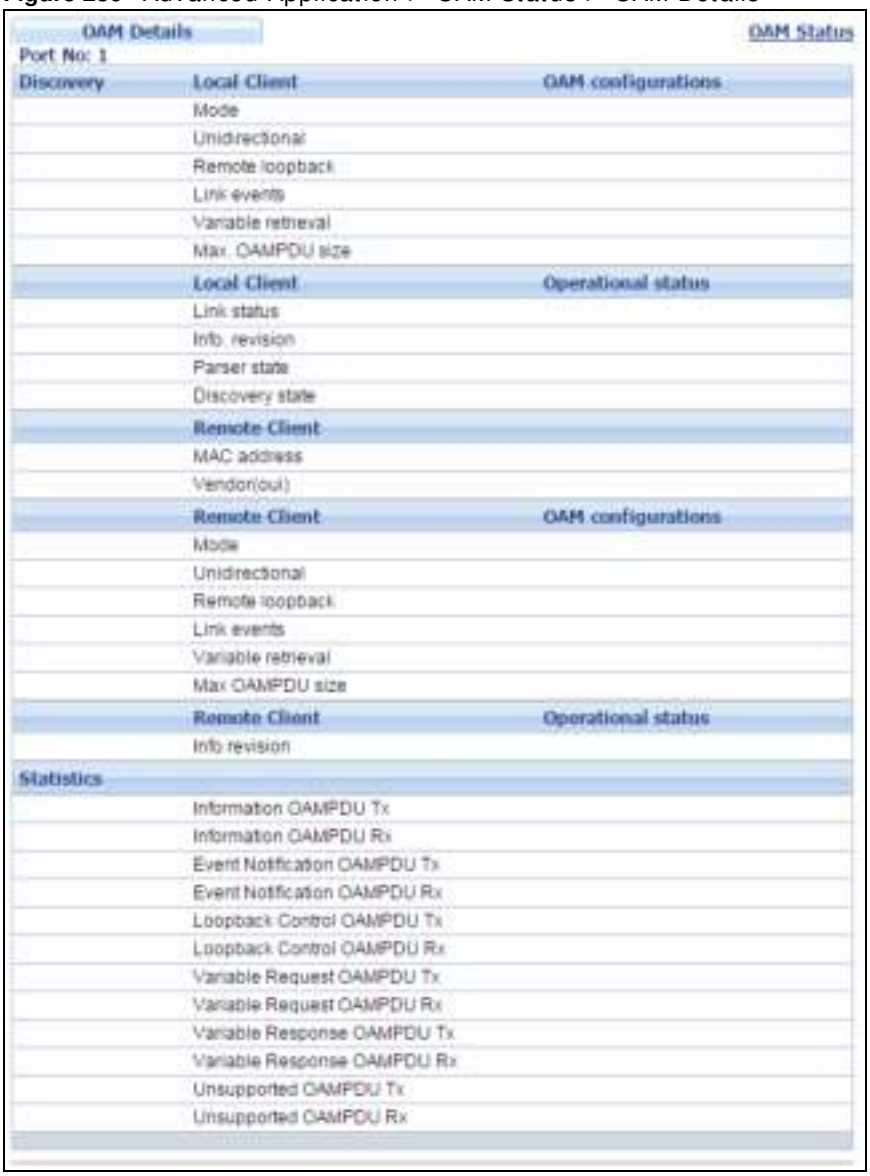
Table 186 Advanced Application > OAM Status

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Local This section displays information about the ports on the Switch.	
Port	This field displays the number of the port on the Switch. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
Mode	This field displays the operational state of the port when OAM is enabled on the port. **Active** - Allows the port to issue and respond to Ethernet OAM commands. **Passive** - Allows the port to respond to Ethernet OAM commands.
Remote This section displays information about the remote device.	
Mac Address	This field displays the MAC address of the remote device.
OUI	This field displays the OUI (first three bytes of the MAC address) of the remote device.
Mode	This field displays the operational state of the port when OAM is enabled on the port. **Active** - Allows the port to issue and respond to Ethernet OAM commands. **Passive** - Allows the port to respond to Ethernet OAM commands.
Config	This field displays the capabilities of the Switch and remote device.

38.2.1 OAM Details

Use this screen to view OAM configuration details and operational status of a specific port. Click a number in the **Port** column in the **OAM Status** screen to display the screen as shown next.

Figure 280 Advanced Application > OAM Status > OAM Details



The following table describes the fields in the above screen.

Table 187 Advanced Application > OAM Status > OAM Details

LABEL	DESCRIPTION
Discovery	This section displays OAM configuration details and operational status of the port on the Switch and/or the remote device.
Local Client/Remote Client OAM configurations	

Table 187 Advanced Application > OAM Status > OAM Details

LABEL	DESCRIPTION
Mode	This field displays the OAM mode. The device in active mode (typically the service provider's device) controls the device in passive mode (typically the subscriber's device). **Active**: The port initiates OAM discovery; sends information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs. **Passive**: The port waits for the remote device to initiate OAM discovery; sends information PDUs; may send event notification PDUs; and may respond to variable request PDUs or loopback control PDUs. The Switch might not support some types of PDUs, as indicated in the fields below.
Unidirectional	This field indicates whether or not the port can send information PDUs to transmit fault information when the receive path is non-operational.
Remote loopback	This field indicates whether or not the port can use loopback control PDUs to put the remote device into loopback mode.
Link events	This field indicates whether or not the port can interpret link events, such as link fault and dying gasp. Link events are sent in event notification PDUs and indicate when the number of errors in a given interval (time, number of frames, number of symbols, or number of errored frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well.
Variable retrieval	This field indicates whether or not the port can respond to requests for more information, such as requests for Ethernet counters and statistics, about link events.
Max. OAMPDU size	This field displays the maximum size of PDU for receipt and delivery.
Local Client/Remote Client OAM configurations	
Link status	This field indicates that the link between the Switch port and a connected IEEE 802.3ah-enabled remote Ethernet device is up or down.
Info. revision	This field displays the current version of local state and configuration. This two-octet value starts at zero and increments every time the local state or configuration changes.
Parser state	This field indicates the current state of the parser. **Forward**: The port is forwarding packets normally. **Loopback**: The port is in loopback mode. **Discard**: The port is discarding non-OAMPDUs because it is trying to or has put the remote device into loopback mode.

Table 187 Advanced Application > OAM Status > OAM Details

LABEL	DESCRIPTION
Discovery state	This field indicates the state in the OAM discovery process. OAM-enabled devices use this process to detect each other and to exchange information about their OAM configuration and capabilities. OAM discovery is a handshake protocol. **Fault**: One of the devices is transmitting OAM PDUs with link fault information, or the interface is not operational. **Active Send Local**: The port is in active mode and is trying to see if the remote device supports OAM. **Passive Wait**: The port is in passive mode and is waiting for the remote device to begin OAM discovery. **Send Local Remote**: This state occurs in the following circumstances. • The port has discovered the remote device but has not accepted or rejected the connection yet. • The port has discovered the remote device and rejected the connection. **Send Local Remote OK**: The port has discovered the remote device and has accepted the connection. In addition, the remote device has not accepted or rejected the connection yet, or the remote device has rejected the connected. **Send Any**: The port and the remote device have accepted the connection. This is the operating state for OAM links that are fully operational.
Statistics This section displays the number of OAM packets transferred on the port of the Switch.	
Information OAMPDU Tx	This field displays the number of OAM PDUs sent on the port.
Information OAMPDU Rx	This field displays the number of OAM PDUs received on the port.
Event Notification OAMPDU Tx	This field displays the number of unique or duplicate OAM event notification PDUs sent on the port.
Event Notification OAMPDU Rx	This field displays the number of unique or duplicate OAM event notification PDUs received on the port.
Loopback Control OAMPDU Tx	This field displays the number of loopback control OAM PDUs sent on the port.
Loopback Control OAMPDU Rx	This field displays the number of loopback control OAM PDUs received on the port.
Variable Request OAMPDU Tx	This field displays the number of OAM PDUs sent to request MIB objects on the remote device.
Variable Request OAMPDU Rx	This field displays the number of OAM PDUs received requesting MIB objects on the Switch.
Variable Response OAMPDU Tx	This field displays the number of OAM PDUs sent by the Switch in response to requests.
Variable Response OAMPDU Rx	This field displays the number of OAM PDUs sent by the remote device in response to requests.
Unsupported OAMPDU Tx	This field displays the number of unsupported OAM PDUs sent on the port.
Unsupported OAMPDU Rx	This field displays the number of unsupported OAM PDUs received on the port.

38.3 OAM Configuration

Use this screen to turn on Ethernet OAM on the Switch and port(s) and configure the related settings.

In the **OAM Status** screen click **Configuration** to display the configuration screen as shown.

Figure 281 Advanced Application > OAM > OAM Configuration (Standalone mode)

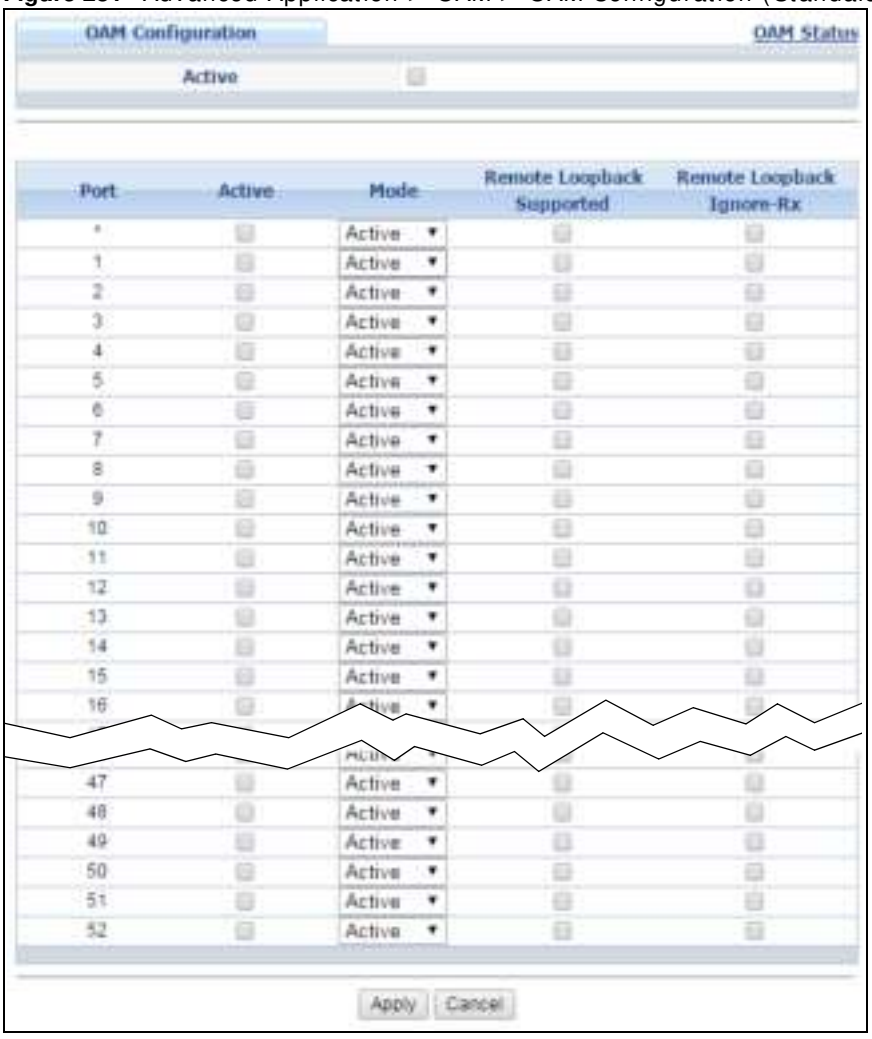
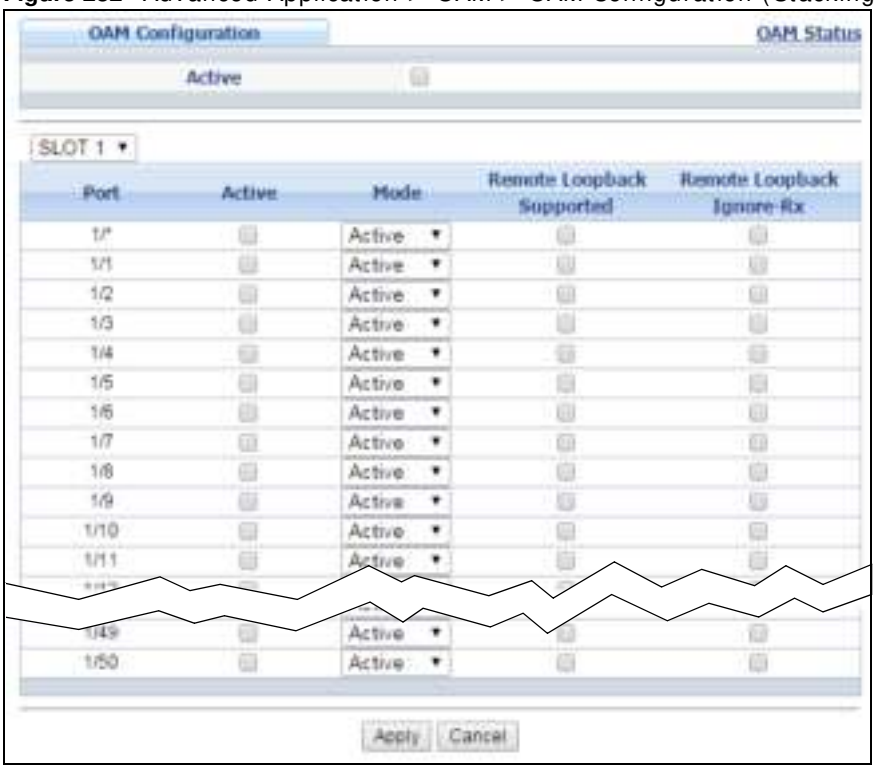


Figure 282 Advanced Application > OAM > OAM Configuration (Stacking mode)



The following table describes the fields in the above screen.

Table 188 Advanced Application > OAM > OAM Configuration

LABEL	DESCRIPTION
Active	Select this option to enable Ethernet OAM on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This field displays the Switch's port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
*	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.
Active	Select this check box to enable Ethernet OAM on this port. Clear this check box to disable Ethernet OAM on the port.
Mode	Specify the OAM mode on the port. Select **Active** to allow the port to issue and respond to Ethernet OAM commands. Select **Passive** to allow the port to respond to Ethernet OAM commands.
Remote Loopback Supported	Select this check box to enable the remote loopback feature on the port. Otherwise, clear the check box to disable it.
Remote Loopback Ignore-Rx	Select this check box to set the Switch to process loopback commands received on the port. Otherwise, clear the check box to have the Switch ignore loopback commands received on the port.

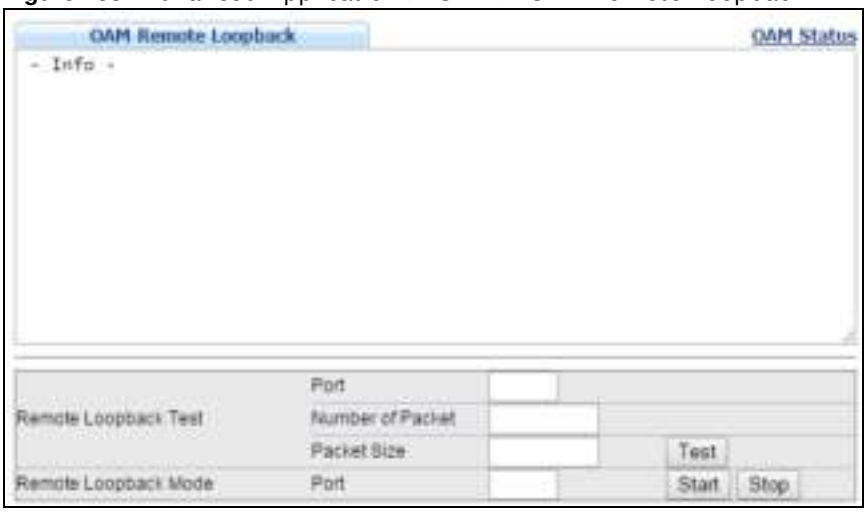
Table 188 Advanced Application > OAM > OAM Configuration

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38.4 OAM Remote Loopback

Use this screen to perform a remote-loopback test. In the **OAM Status** screen click **Remote Loopback** to display the screen as shown.

Figure 283 Advanced Application > OAM > OAM Remote Loopback



The following table describes the fields in the above screen.

Table 189 Advanced Application > OAM > OAM Remote Loopback

LABEL	DESCRIPTION
Remote Loopback Test	
Port	Enter the number of the port from which the Switch performs a remote-loopback test.
Number of Packet	Define the allowable packet number of the loopback test frames.
Packet Size	Define the allowable packet size of the loopback test frames.
Test	Click **Test** to begin the test.
Remote Loopback Mode	
Port	Enter the number of the port from which the Switch sends loopback control PDUs to initiate or terminate a remote-loopack test.
Start	Click **Start** to initiate a remote-loopback test from the specified port by sending Enable Loopback Control PDUs to the remote device.
Stop	Click **Stop** to terminate a remote-loopback test from the specified port by sending Disable Loopback Control PDUs to the remote device.

39

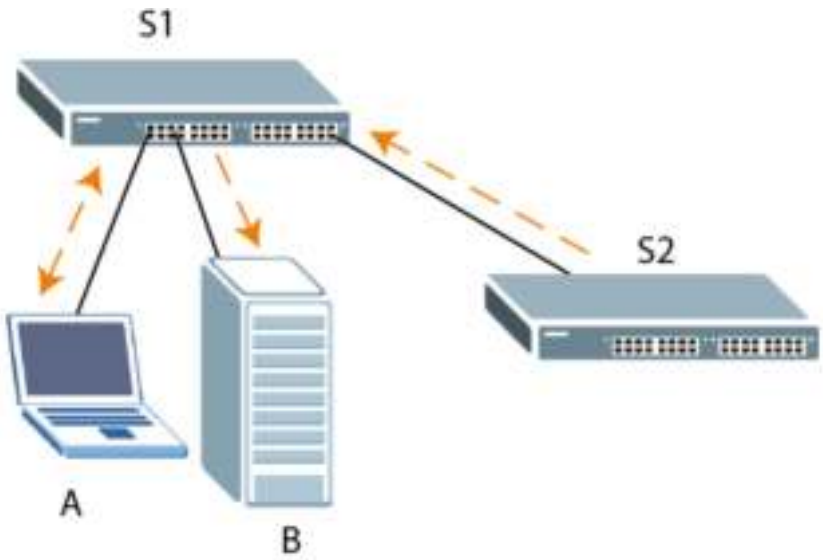
ZULD

39.1 ZULD Overview

A unidirectional link is a connection where the link is up on both ends, but only one end can receive packets. This may happen if OAM was initially enabled but then disabled, there are misconfigured transmitting or receiving lines or the hardware is malfunctioning. ZyXEL Unidirectional Link Detection (**ZULD**) is a layer-2 protocol that can detect and disable these physical one-way links before they cause loops or communication malfunction.

In the figure below, S1 - A is a bidirectional link as both ends can send packets to each other. S1-B is unidirectional as B cannot send packets to S1 (although the S1-B link is up). Similarly, S2-S1 is unidirectional as S1 cannot send packets to S2 (although the S1-S2 link is up).

Figure 284 ZULD Overview



39.1.1 What You Can Do

- Use the **ZULD Status** screen (Section 39.2 on page 391) to see details on ZULD.
- Use the **ZULD Configuration** screen (Section 39.3 on page 393) to enable ZULD on a port, configure a mode and set the probe time.

39.1.2 What You Need to Know

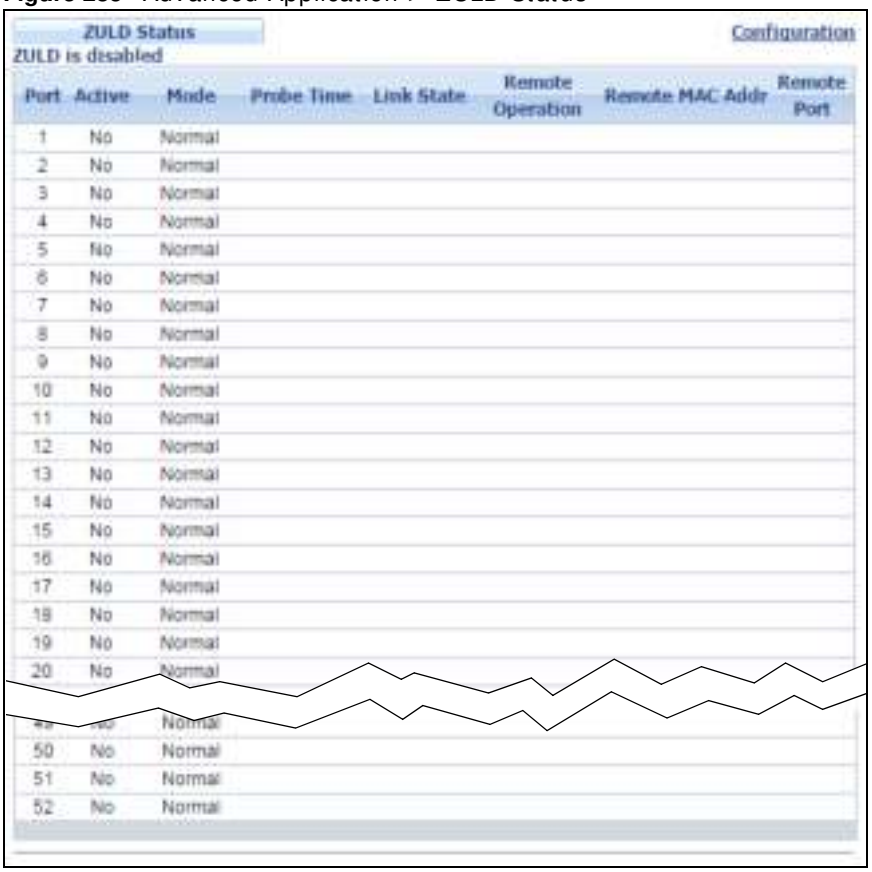
- ZULD must be enabled on the Switch and the port(s) in order to detect unidirectional links by monitoring OAMPDUs.

- Ports advertise their unidirectional link detection capability using OAMPDUs, so all connected devices must support **OAM** as well as **ZULD**. You need to enable OAM on the Switch by going to **Advanced Application > OAM > Configuration** and selecting **Active**. OAM must be enabled on other connected devices too. If OAM is not enabled initially, **ZULD** will not work.
- If OAM is enabled initially and later disabled on one end of a link, the link will be unidirectional as that end cannot send OAMPDUs.
- OAM discovery, the sending of OAMPDUs to other ports, is initiated by an active port.
- When **ZULD** detects a unidirectional link, it sends a syslog and SNMP trap and may shut down the affected port (**Aggresssive Mode**).
- If a port on the Switch is shut down by **ZULD**, and you want to recover it, then do one of the following:
  - Go to **Basic Setting > Port Setup**. Clear **Active** and click **Apply**. Then select **Active** and click **Apply** again.
  - Go to **Application > Errdiable > Errdisable Recovery** and set the interval for **ZULD**. After the interval expires, the closed port(s) will become active and start receiving packets again.
  - Use the command `port no inactive`.
- Refer to the ZULD logs to see when a unidirectional link is detected and when it is recovered to a bidirectional link.

39.2 ZULD Status

Use this screen to see details of unidirectional and bidirectional links discovered by **ZULD**. To open this screen, click **Advanced Application > ZULD**.

Figure 285 Advanced Application > ZULD Status



The following table describes the fields in the above screen.

Table 190 Advanced Application > ZULD Status

LABEL	DESCRIPTION
ZULD is....	This shows whether **ZULD** is enabled or disabled on the Switch.
Port	This field displays the port number of the Switch.
Active	This field displays whether ZULD is enabled on the port or not. ZULD must be enabled to detect an unidirectional link by monitoring OAMPDUs.
Mode	This field indicates what **ZULD** will do when a unidirectional link is detected. In **Normal** mode, **ZULD** only sends a syslog and trap when it detects a unidirectional link. In **Aggressive** mode, **ZULD** shuts down the port (puts it into an **ErrDisable** state) as well as sends a syslog and trap when it detects a unidirectional link.
Probe Time	Probe time is the length of time that **ZULD** waits before declaring that a link is unidirectional. When the probe time expires, and one port (either on the Switch or the connected device) still has not received an OAMPDU, then **ZULD** declares that the link is unidirectional.

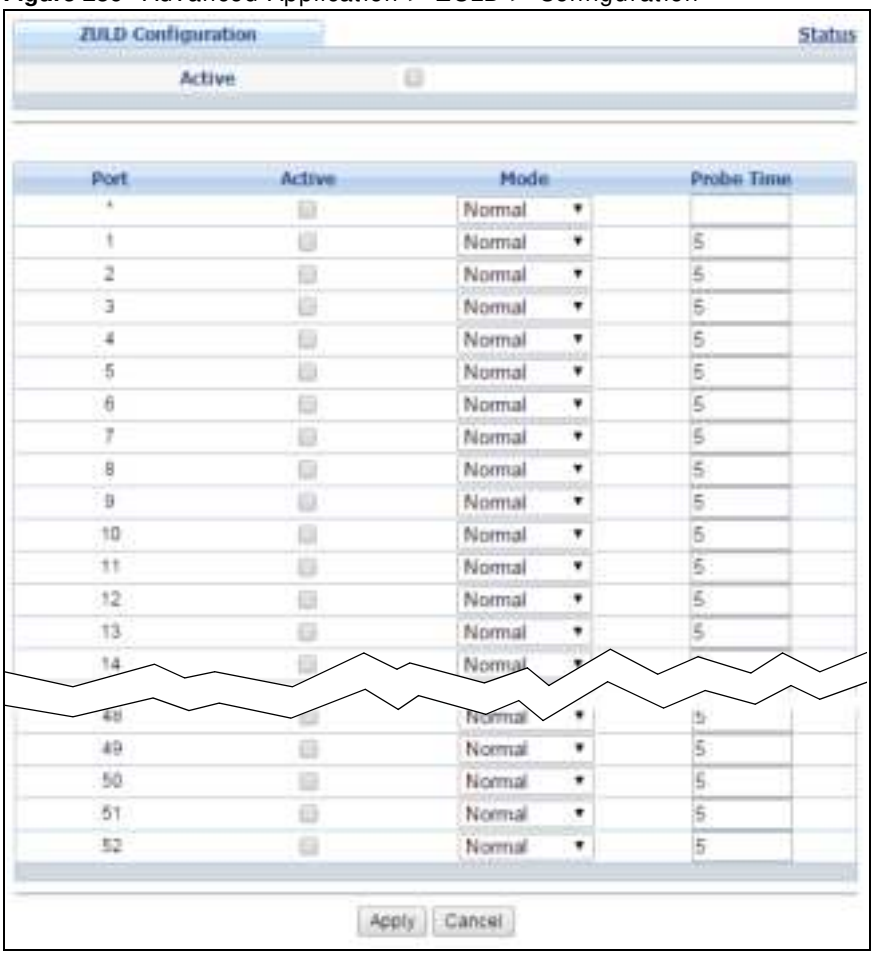
Table 190 Advanced Application > ZULD Status

LABEL	DESCRIPTION
Link State	This field shows the following link states: • **Linkdown**: This is an initialization state, where the port is not yet up. • **Probe**: This indicates that **ZULD** is discovering the connected device on this link. • **Bidirectional**: Traffic sent by the Switch is received by the connected device on this link, and traffic from the connected device on this link is received by the Switch. • **Unidirectional**: The state of the link between the port and its connected port cannot be determined either because no ZULD message was received, or one port is not capable of sending traffic. • **Shutdown**: The port has been shut down because its link with the connected device is unidirectional and **ZULD** is in **Aggressive** mode.
Remote Operation	This field displays whether ZULD is enabled or disabled on the connected device on this link. ZULD must be enabled on the connected device and on the port that's connecting to the Switch.
Remote MAC Addr	This is the MAC address of the port on the connected device to which the port of the Switch is connected.
Remote Port	This is the port number of the port on the connected device to which the port of the Switch is connected.

39.3 ZULD Configuration

Use this screen to enable ZULD on a port, configure a mode and set the probe time. To open this screen, click **Advanced Application > ZULD > Configuration**.

Figure 286 Advanced Application > ZULD > Configuration



The following table describes the fields in the above screen.

Table 191 Advanced Application > ZULD > Configuration

LABEL	DESCRIPTION
Active	Select this to enable **ZULD** on the Switch.
Port	Use port * to configure all ports to have the same settings. Alternatively, select individual ports for different settings.
Active	Select this to enable **ZULD** on the port. ZULD must be enabled to detect an unidirectional link by monitoring OAMPDUs.
Mode	Select **Normal** or **Aggressive**. In **Normal** mode, ZULD only sends a syslog and trap when it detects a unidirectional link. In **Aggressive** mode, ZULD shuts down the port (puts it into an **ErrDisable** state) as well as sends a syslog and trap when it detects a unidirectional link.
Probe Time	Type the length of time that **ZULD** waits before declaring that a link is unidirectional. When the probe time expires, and one port (either on the Switch or the connected device) still has not received an OAMPDU, then **ZULD** declares that the link is unidirectional. The allowed time range is from 5-65535 seconds.

Table 191 Advanced Application > ZULD > Configuration

LABEL	DESCRIPTION
Apply	Click **Apply** 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 **Save** 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.

40

Static Route

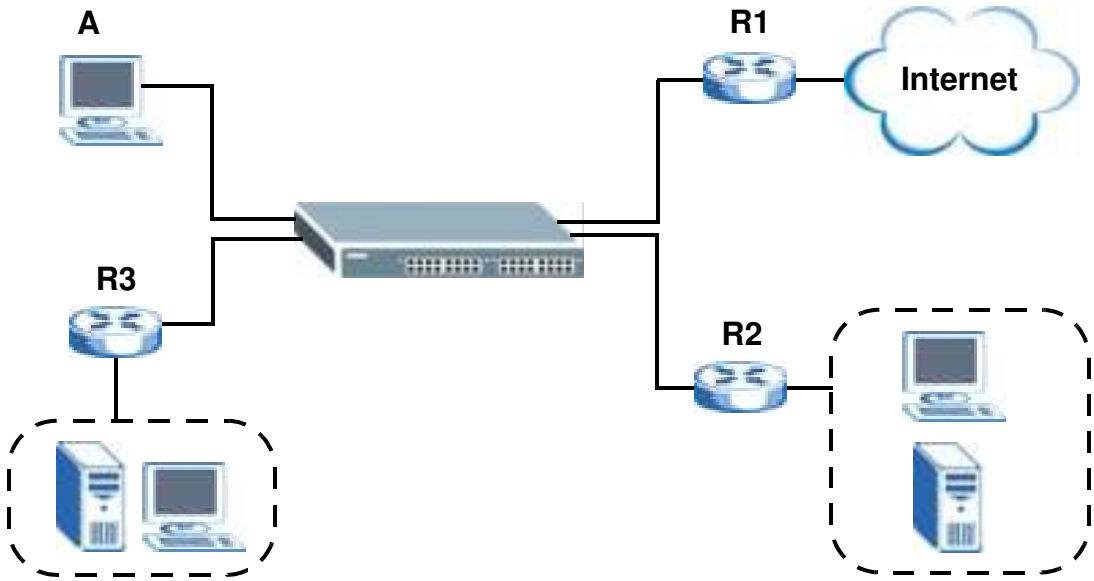
This chapter shows you how to configure static routes.

40.1 Static Routing Overview

The Switch usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Switch send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Switch. The Switch routes most traffic from **A** to the Internet through the Switch's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the Switch.

Figure 287 Example of Static Routing Topology



40.2 Static Routing

Click **IP Application** > **Static Routing** in the navigation panel to display the screen as shown. Click the link next to **IPv4 Static Route** to open a screen where you can create IPv4 static routing rules. Click the link next to **IPv6 Static Route** to open a screen where you can create IPv6 static routing rules.

Figure 288 IP Application > Static Routing

40.3 Configuring IPv4 Static Routing

Click the link next to **IPv4 Static Route** in the **IP Application** > **Static Routing** screen to display the screen as shown.

Figure 289 IP Application > Static Routing > IPv4 Static Route

The following table describes the related labels you use to create a static route.

Table 192 IP Application > Static Routing > IPv4 Static Route

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. 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.
IP Subnet Mask	Enter the subnet mask for this destination.
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.

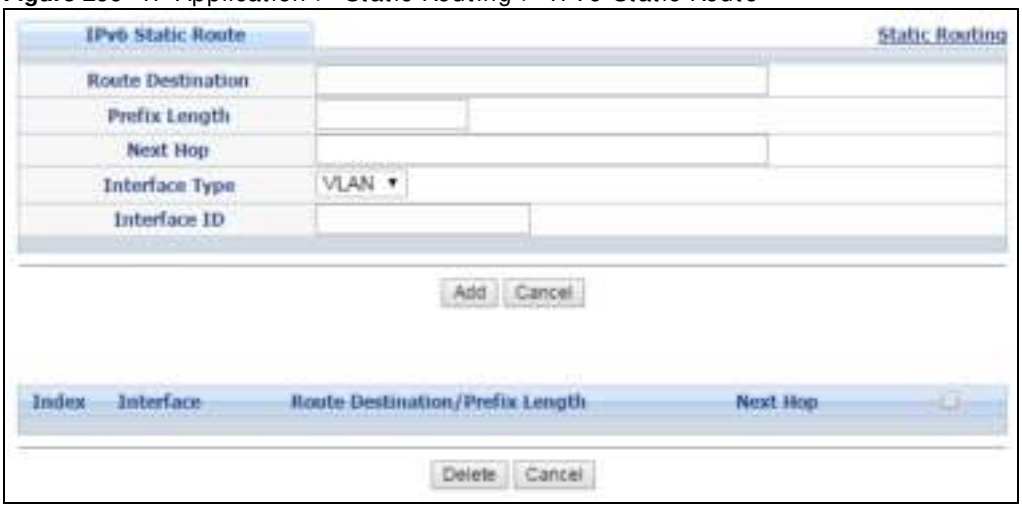
Table 192 IP Application > Static Routing > IPv4 Static Route (continued)

LABEL	DESCRIPTION
Add	Click **Add** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** 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 **Yes** when the static route is activated and **NO** 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.
Gateway Address	This field displays the IP address of the gateway. The gateway is the immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

40.4 Configuring IPv6 Static Routing

Click the link next to **IPv6 Static Route** in the **IP Application** > **Static Routing** screen to display the screen as shown.

Figure 290 IP Application > Static Routing > IPv6 Static Route



The following table describes the related labels you use to create a static route.

Table 193 IP Application > Static Routing > IPv6 Static Route

LABEL	DESCRIPTION
Route Destination	Enter the IPv6 address of the final destination.
Prefix Length	Enter the prefix length number of up to 64 for this destination.
Next Hop	Enter the IPv6 address of the next-hop router.
Interface Type	Select the type of the IPv6 interface through which the IPv6 packets are forwarded. The Switch supports only the VLAN interface type at the time of writing.
Interface ID	Enter the ID number of the IPv6 interface through which the IPv6 packets are forwarded.
Add	Click **Add** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Interface	This field displays the descriptive name of the interface that is used to forward the packets to the destination.
Route Destination/ Prefix Length	This field displays the IPv6 subnet prefix and prefix length of the final destination.
Next Hop	This field displays the IPv6 address of the gateway that helps forward the packet to the destination.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

41

Policy Routing

This chapter shows you how to configure policy routing rules.

41.1 Policy Route Overview

Traditionally, routing is based on the destination address only and the Switch takes the shortest path to forward a packet. Policy routing provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets prior to the normal routing.

Individual routing policies are used as part of the overall policy routing process. A routing policy defines the action to take when a packet meets the criteria in a specified classifier. The action is taken only when all the criteria are met.

41.1.1 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Cost Savings – Policy routing allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use policy routing to distribute traffic among multiple paths.

41.2 Configuring Policy Routing Profile

Click **IP Application** > **Policy Routing** in the navigation panel to display the screen as shown. Use this screen to configure a policy routing profile, which can consist of multiple policy routing rules.

Figure 291 IP Application > Policy Routing

The following table describes the labels in this screen.

Table 194 IP Application > Policy Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this policy routing profile and rules in the profile.
Profile Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes. Spaces are allowed.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of the policy routing profile. Click a number to edit the policy routing profile entry.
Active	This field displays **Yes** when the policy routing profile is activated and **No** when it is deactivated.
Profile Name	This field displays the descriptive name for this profile. This is for identification purposes only.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

41.2.1 Policy Routing Rule Configuration

You must first configure a layer-3 classifier in the **Classifier** screen (see Section 19.2 on page 201) and a policy routing profile in the **Policy Routing** screen (see Section 41.2 on page 400).

Use this screen to configure a policy route to override the default (shortest path) routing behavior and forward packets based on the classifier and action you specify. A policy route rule defines the matching classifier and the action to take when a packet meets the criteria in the classifier. The action is taken only when all the criteria are met. Policy-based routing is applied to incoming packets on a per interface basis before normal routing. The Switch does not perform normal routing on packets that match any of the policy routes.

Click **Rule Configuration** in the **IP Application** > **Policy Routing** screen to display the screen as shown.

Figure 292 IP Application > Policy Routing > Rule Configuration

The following table describes the labels in this screen.

Table 195 IP Application > Policy Routing > Rule Configuration

LABEL	DESCRIPTION
Profile Name	This field displays the policy routing profile(s) you configure in the **IP Application > Policy Routing** screen. Select a profile for which you want to configure a policy routing rule.
Sequence	Enter the rule number from 1 to 64. The ordering of your rules is important as rules are applied in turn. You can not specify a number already in use by another rule.
Statement	Select **Permit** to forward traffic that matches this rule to the gateway specified in the rule. Select **Deny** to disable the rule action and forward traffic that matches this rule according to the routing table on the Switch.
Classifier	This field displays the available active classifiers you configure in the **Classifier** screen (see Chapter 19 on page 201), which are not used by any policy rule or policy routing rule. Select a classifier to which this policy routing rule applies.
Action	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Active	This field displays whether the policy route profile is enabled or not.
Profile Name	This field displays the name of the policy route profile with which the rule is associated.

Table 195 IP Application > Policy Routing > Rule Configuration (continued)

LABEL	DESCRIPTION
Seq	This field displays the rule index number that you configure in the **Sequence** field. Click an index number to change the rule's **Statement**.
State	This field displays **permit** when the rule action is activated and **deny** when is it deactivated.
Classifier	This field displays the name of the classifier to which this policy applies.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry(ies) from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

42

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

42.1 DiffServ Overview

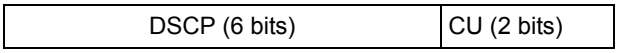
Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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.

42.1.1 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 293 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.

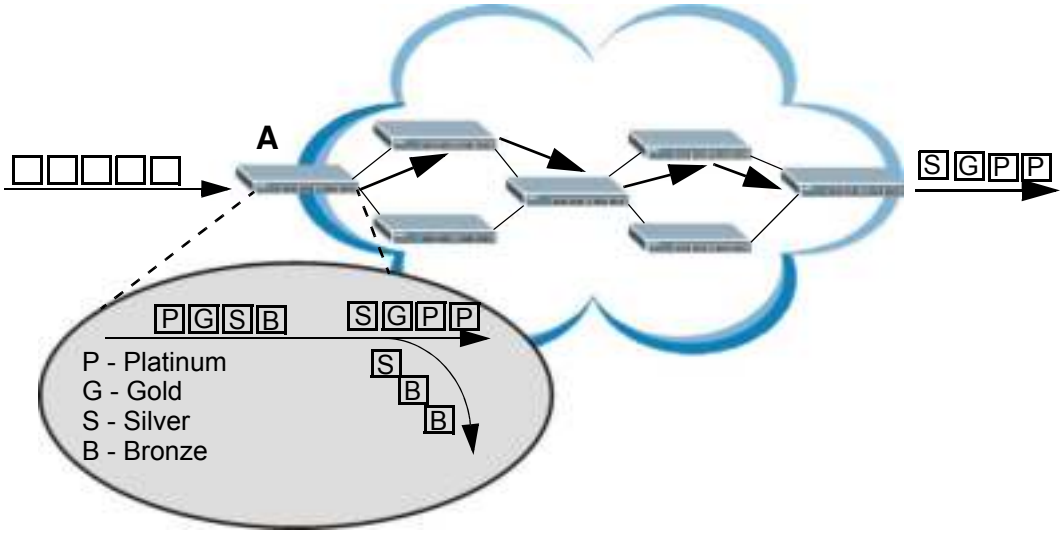
The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

42.1.2 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 294) 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. For example, one traffic policy would be 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 294 DiffServ Network



42.2 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:

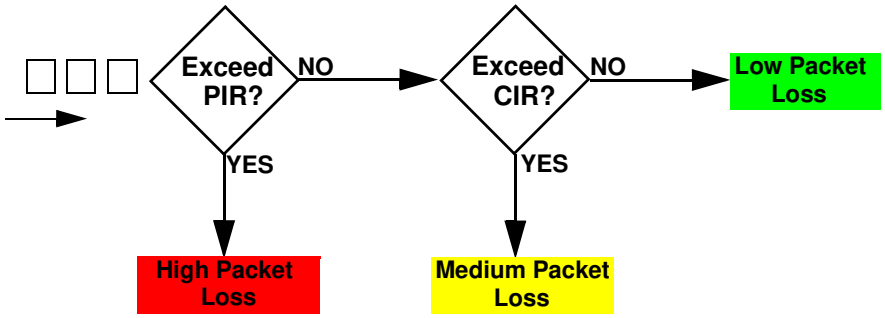
- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.
- Green (low loss priority level) packets are forwarded.

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.

42.2.1 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 295 TRTCM - Color-blind Mode

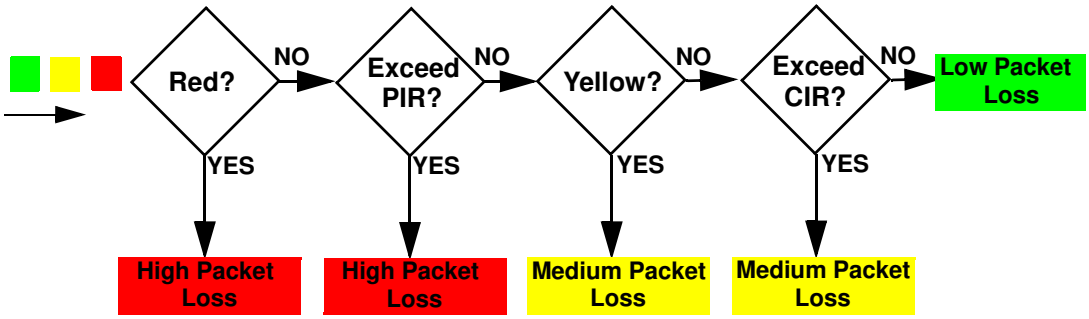


42.2.2 TRTCM - Color-aware Mode

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 296 TRTCM - Color-aware Mode



42.3 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 297 IP Application > DiffServ (Standalone mode)

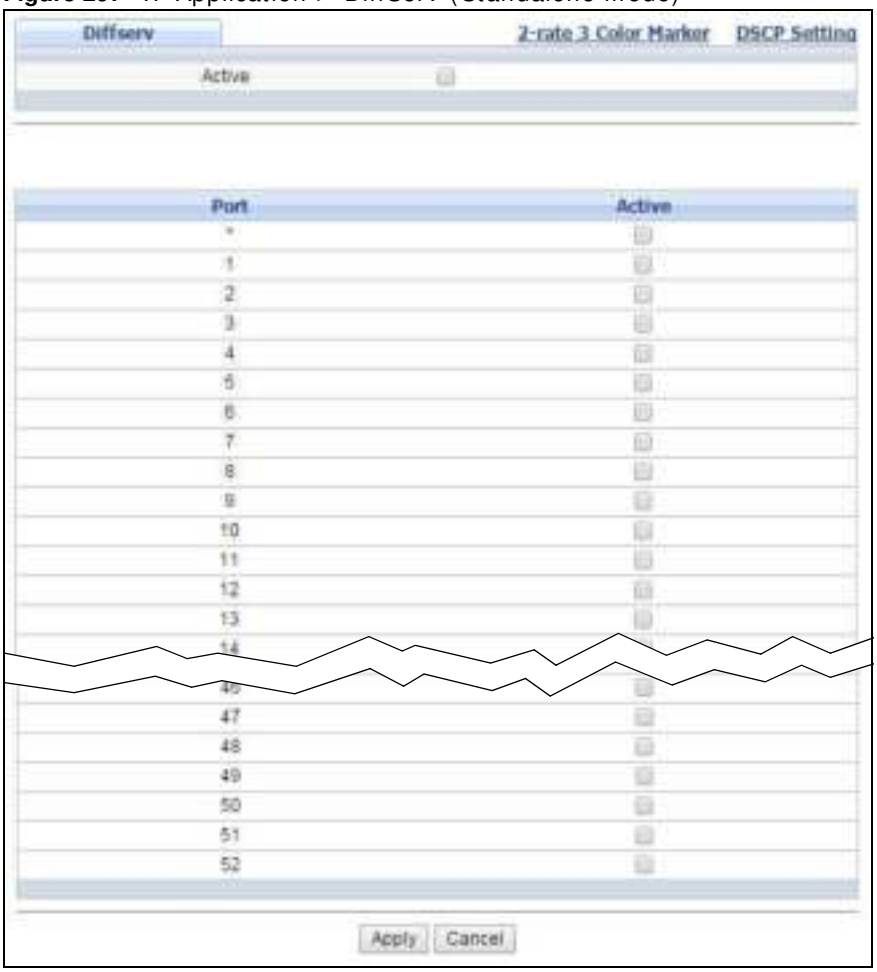
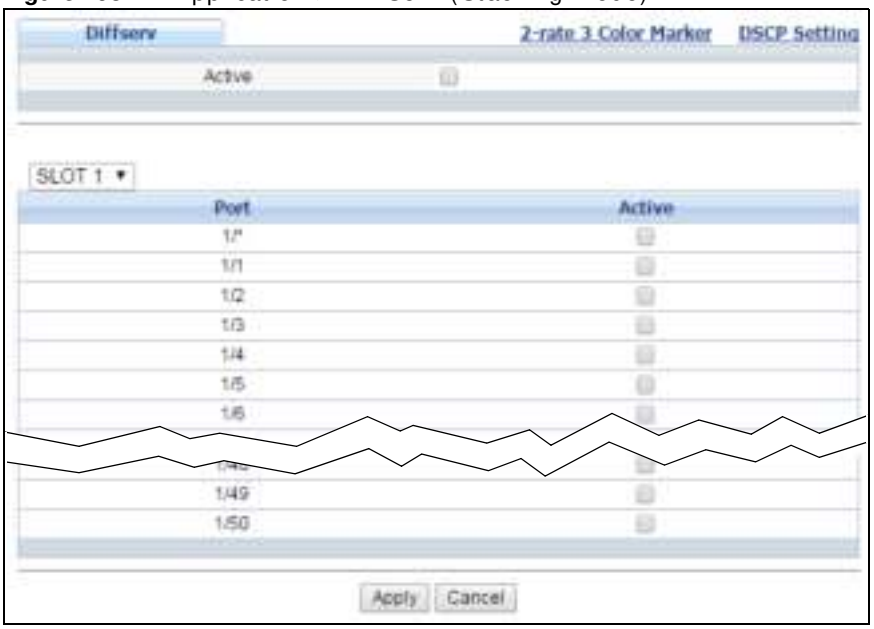


Figure 298 IP Application > DiffServ (Stacking mode)



The following table describes the labels in this screen.

Table 196 IP Application > DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This field displays the index number of a port on the Switch. In stacking mode, the first number represents the slot and the second the port number. * means all ports (on the same 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 **Active** to enable DiffServ on the port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

42.3.1 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 299 IP Application > DiffServ > 2-rate 3 Color Marker (Standalone mode)

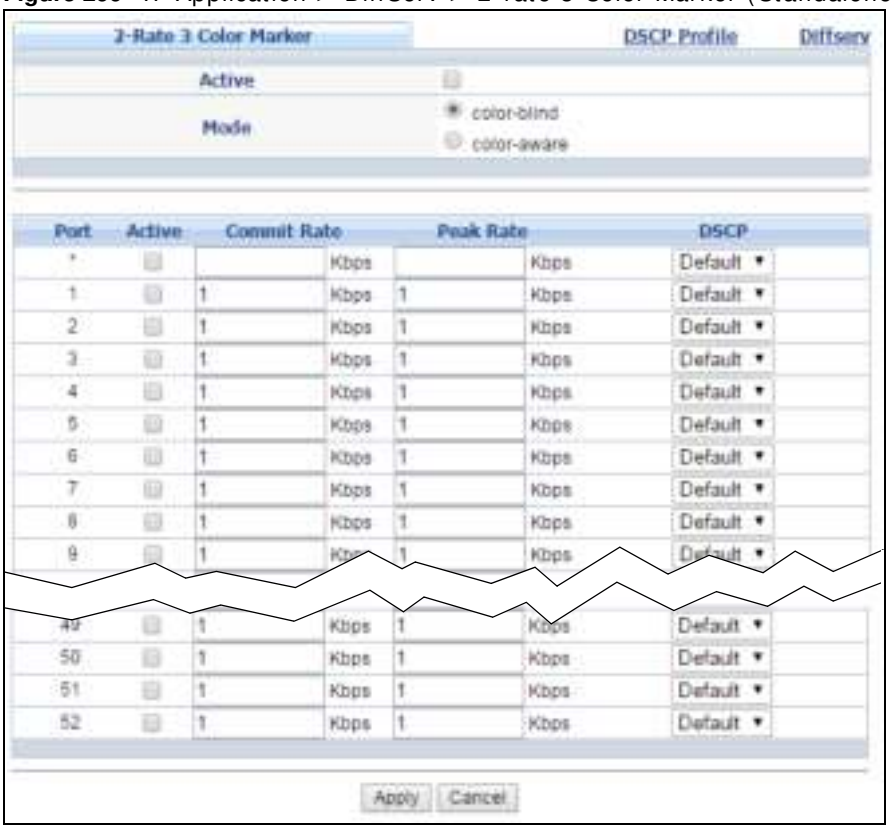
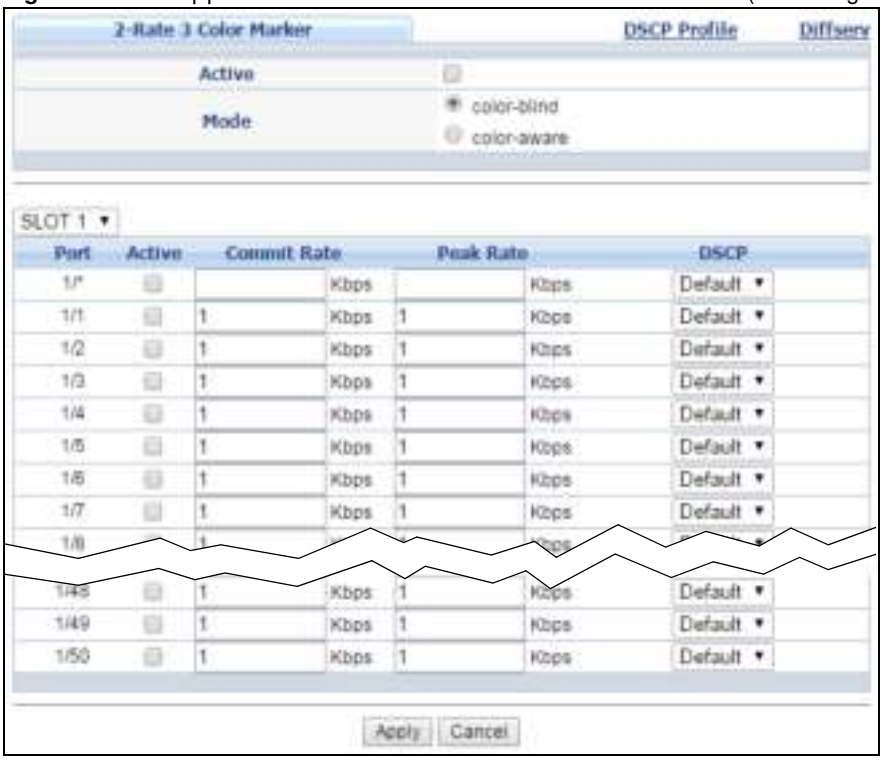


Figure 300 IP Application > DiffServ > 2-rate 3 Color Marker (Stacking mode)



The following table describes the labels in this screen.

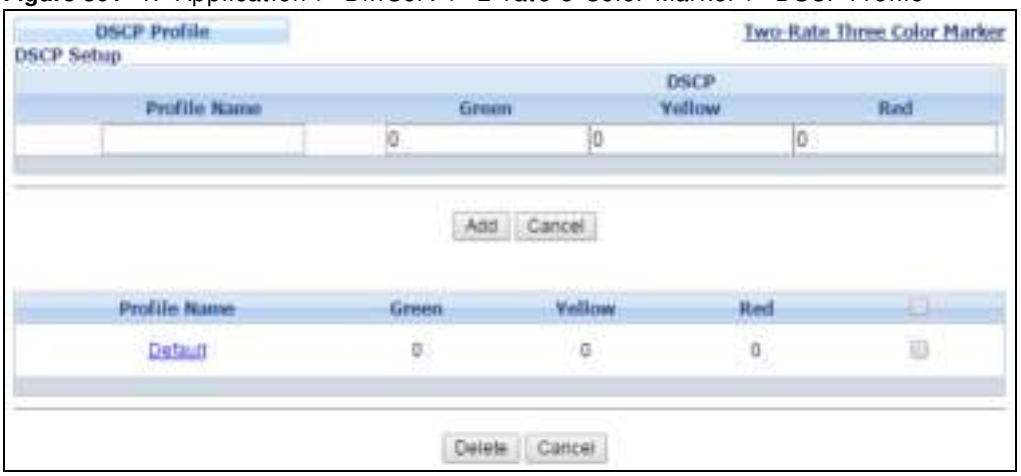
Table 197 IP Application > DiffServ > 2-rate 3 Color Marker

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 **DiffServ** on the Switch and the individual ports for the Switch to drop red (high loss priority) colored packets.
Mode	Select **color-blind** to have the Switch treat all incoming packets as uncolored. All incoming packets are evaluated against the CIR and PIR. Select **color-aware** 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.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This field displays the index number of a port on the Switch. In stacking mode, the first number represents the slot and the second the port number. * means all ports (on the same 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	Select a pre-defined DSCP profile. The Switch assigns the DSCP values defined in the profile to packets based on the color they are marked via TRTCM.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

42.3.2 DSCP Profile

Use this screen to create DSCP profiles. To open this screen, click the **DSCP Profile** link in the **IP Application > DiffServ > 2-rate 3 Color Marker** screen.

Figure 301 IP Application > DiffServ > 2-rate 3 Color Marker > DSCP Profile



The following table describes the labels in this screen.

Table 198 IP Application > DiffServ > 2-rate 3 Color Marker > DSCP Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes.
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.
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.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** 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 fields to your previous configuration.
Profile Name	This field displays the descriptive name of the profile. Click the profile name to change the settings.
Green	This field displays the DSCP value to use for packets with low packet loss priority.
Yellow	This field displays the DSCP value to use for packets with medium packet loss priority.
Red	This field displays the DSCP value to use for packets with high packet loss priority.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click the **Delete** button to remove the selected entry(ies) from the table.
Cancel	Click this to revert the fields to the previous configuration.

42.4 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 199 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

42.4.1 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 302 IP Application > DiffServ > DSCP Setting

The following table describes the labels in this screen.

Table 200 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.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

43

DHCP

This chapter shows you how to configure the DHCP feature.

43.1 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 server or a DHCP relay agent. When configured as a server, the Switch provides the TCP/IP configuration for the clients. 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 server or 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.

43.1.1 DHCP Modes

The Switch can be configured as a DHCP server or DHCP relay agent.

- If you configure the Switch as a DHCP server, it will maintain the pool of IP addresses along with subnet masks, DNS server and default gateway information and distribute them to your LAN computers.
- 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.

43.1.2 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 as a DHCP server for one VLAN and at the same time the Switch can be configured to relay DHCP requests for clients in another VLAN.

43.2 DHCP Configuration

Click **IP Application** > **DHCP** in the navigation panel to display the screen as shown. Click the link next to **DHCPv4** to open screens where you can enable and configure DHCPv4 server/relay settings

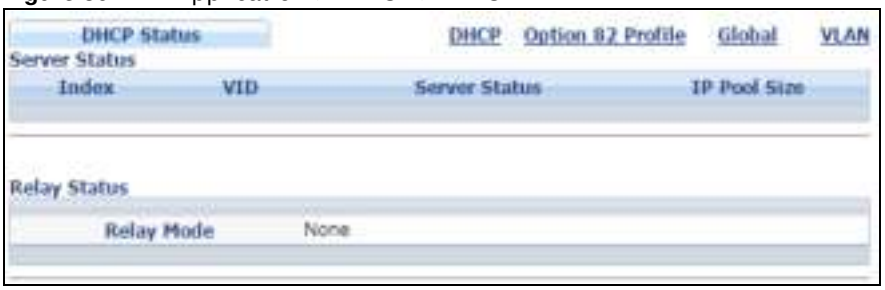
and create option 82 profiles. Click the link next to **DHCPv6** to open screens where you can configure DHCPv6 settings.

Figure 303 IP Application > DHCP

43.3 DHCPv4 Status

Click **IP Application** > **DHCP** > **DHCPv4** in the navigation panel. The **DHCP Status** screen displays.

Figure 304 IP Application > DHCP > DHCPv4



The following table describes the labels in this screen.

Table 201 IP Application > DHCP > DHCPv4

LABEL	DESCRIPTION
Server Status	This section displays configuration settings related to the Switch's DHCP server mode.
Index	This is the index number. Click an index number to change the settings.
VID	This field displays the VLAN ID for which the Switch is a DHCP server.
Server Status	This field displays the starting DHCP client IP address.
IP Pool Size	This field displays the number of IP addresses that can be assigned to clients.
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: • **None** - if the Switch is not configured as a DHCP relay agent. • **Global** - if the Switch is configured as a DHCP relay agent only. • **VLAN** - followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLAN(s).

43.3.1 DHCPv4 Server Status Detail

Click **IP Application** > **DHCP** > **DHCPv4** in the navigation panel and then click an existing index number of a DHCP server configuration to view the screen as shown. Use this screen to view details regarding DHCP server settings configured on the Switch.

Figure 305 IP Application > DHCP > DHCPv4 > Server Status Detail

The following table describes the labels in this screen.

Table 202 IP Application > DHCP > DHCPv4 > Server Status Detail

LABEL	DESCRIPTION
Start IP Address	This field displays the starting IP address of the IP address pool configured for this DHCP server instance.
End IP Address	This field displays the last IP address of the IP address pool configured for this DHCP server instance.
Subnet Mask	This field displays the subnet mask value sent to clients from this DHCP server instance.
Default Gateway	This field displays the default gateway value sent to clients from this DHCP server instance.
Primary DNS Server	This field displays the primary DNS server value sent to clients from this DHCP server instance.
Secondary DNS Server	This field displays the secondary DNS server value sent to clients from this DHCP server instance.
Lease Time	This field displays the amount of time that the IP address is valid.
Address Leases	This section displays information about the IP addresses this DHCP server issued to clients.
Index	This field displays a sequential number for each DHCP request handled by the Switch.
IP Address	This is the IP address issued to a DHCP client.
Timer	This field displays the time remaining before the DHCP client has to renew its IP address.
Hardware Address	This field displays the MAC address of the DHCP client. It may also display **SELF OCCUPIED ADDRESS** if the IP address cannot be used for DHCP because it is already assigned to the Switch itself.
Hostname	This field displays the system name of the client.

43.4 DHCPv4 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.

43.4.1 DHCPv4 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.

43.4.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 203 DHCP Relay Agent Information Option Format

Code (82)	Length (N)	i1	i2	...	iN

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.

43.4.1.2 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 204 DHCP Relay Agent Circuit ID Sub-option Format

SubOpt Code	Length	Value
1 (1 byte)	N (1 byte)	Slot ID, Port ID, VLAN ID, System Name or String

Table 205 DHCP Relay Agent Remote ID Sub-option Format

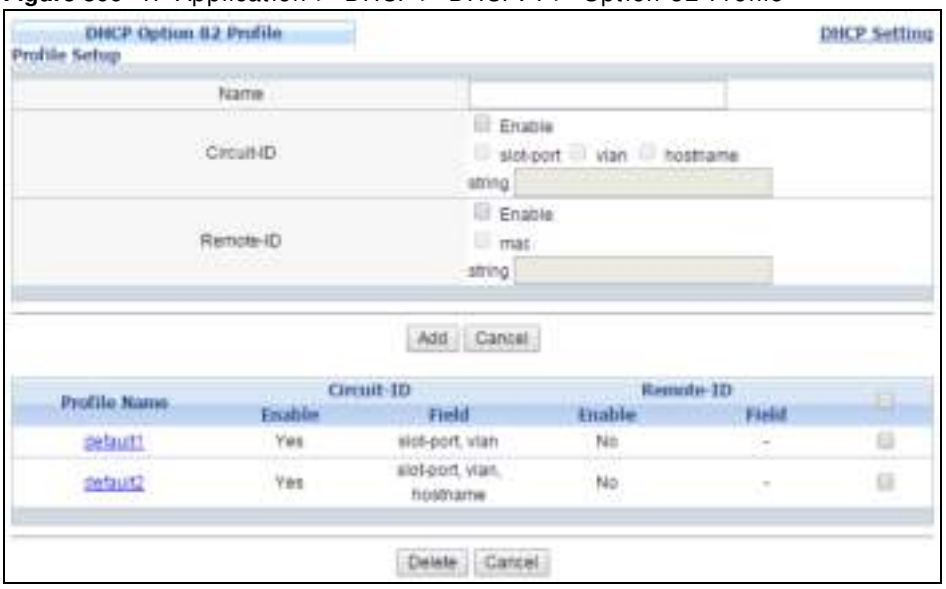
SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	MAC Address or String

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.

43.4.2 DHCPv4 Option 82 Profile

Use this screen to create DHCPv4 option 82 profiles. Click **IP Application > DHCP > DHCPv4** in the navigation panel and click the **Option 82 Profile** link to display the screen as shown.

Figure 306 IP Application > DHCP > DHCPv4 > Option 82 Profile



The following table describes the labels in this screen.

Table 206 IP Application > DHCP > DHCPv4 > Option 82 Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for the profile for identification purposes. You can use up to 32 ASCII characters. Spaces are allowed.
Circuit-ID	Use this section to configure the Circuit ID sub-option to include information that is specific to the relay agent (the Switch).
Enable	Select this option to have the Switch add the Circuit ID sub-option to client DHCP requests that it relays to a DHCP server.
slot-port	Select this option to have the Switch add the number of port that the DHCP client is connected to.
vlan	Select this option to have the Switch add the ID of VLAN which the port belongs to.
hostname	This is the system name you configure in the **Basic Setting** > **General Setup** screen. Select this option for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters that the Switch adds into the client DHCP requests. Spaces are allowed.
Remote-ID	Use this section to configure the Remote ID sub-option to include information that identifies the relay agent (the Switch).
Enable	Select this option to have the Switch append the Remote ID sub-option to the option 82 field of DHCP requests.
mac	Select this option to have the Switch add its MAC address to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters for the remote ID information in this field. Spaces are allowed.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.

Table 206 IP Application > DHCP > DHCPv4 > Option 82 Profile (continued)

LABEL	DESCRIPTION
Profile Name	This field displays the descriptive name of the profile. Click the name to change the settings.
Circuit-ID	
Enable	This field displays whether the Circuit ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Circuit ID sub-option.
Remote-ID	
Enable	This field displays whether the Remote ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Remote ID sub-option.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

43.4.3 Configuring DHCPv4 Global Relay

Use this screen to configure global DHCPv4 relay. Click **IP Application > DHCP > DHCPv4** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 307 IP Application > DHCP > DHCPv4 > Global

The following table describes the labels in this screen.

Table 207 IP Application > DHCP > DHCPv4 > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCPv4 relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCPv4 server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

43.4.4 DHCPv4 Global Relay Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports on the Switch. To open this screen, click **IP Application > DHCP > DHCPv4 > Global > Port**.

Figure 308 IP Application > DHCP > DHCPv4 > Global > Port

The following table describes the labels in this screen.

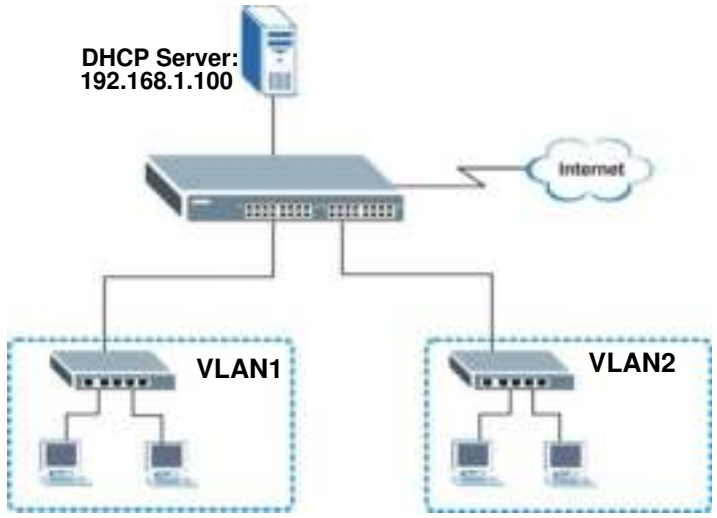
Table 208 IP Application > DHCP > DHCPv4 > Global > Port

LABEL	DESCRIPTION
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s). The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. Note: The profile you select here has priority over the one you select in the **DHCP > DHCPv4 > Global** screen.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** 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 above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
Port	This field displays the port(s) to which the Switch applies the settings. In stacking mode, the first number represents the slot and the second the port number.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s).
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the entry(ies) that you want to remove, then click the **Delete** button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the check boxes above.

43.4.5 Global DHCP Relay Configuration Example

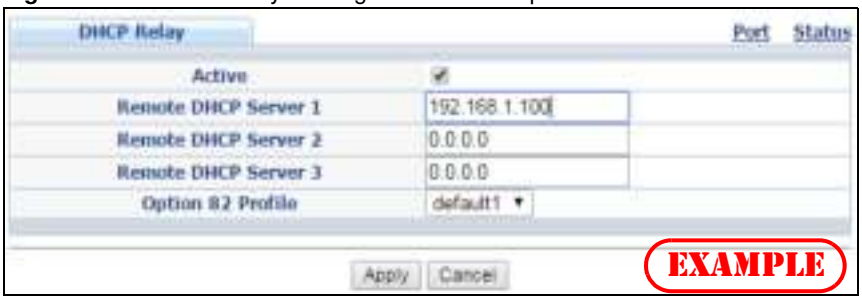
The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 309 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select a DHCP option 82 profile (**default1** in this example) 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 310 DHCP Relay Configuration Example

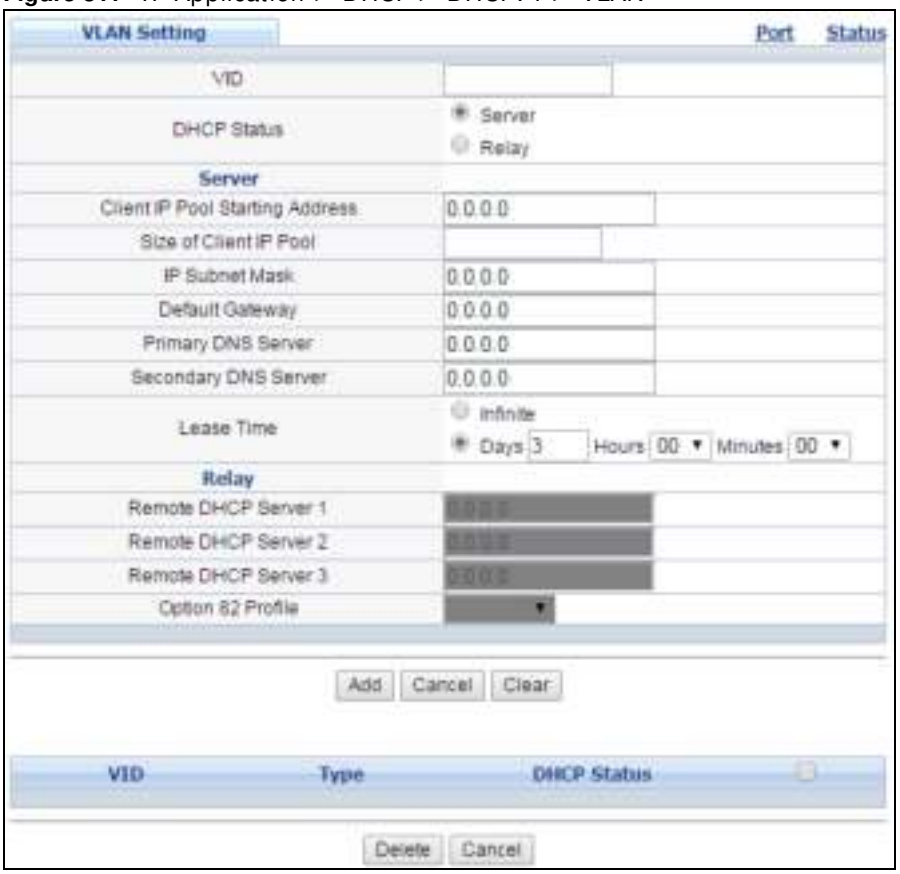


43.5 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP** > **DHCPv4** 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 6.5 on page 65 for information on how to do this.

Figure 311 IP Application > DHCP > DHCPv4 > VLAN



The following table describes the labels in this screen.

Table 209 IP Application > DHCP > DHCPv4 > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
DHCP Status	Select whether the Switch should function as a DHCP **Server** or **Relay** for the specified VID. If you select **Server** then fields related to DHCP relay configuration are grayed out and vice versa.
Server	Use this section if you want to configure the Switch to function as a DHCP server for this VLAN.
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool. The Switch can issue from 1 to 253 IP addresses to DHCP clients.
IP Subnet Mask	Enter the subnet mask for the client IP pool.
Default Gateway	Enter the IP address of the default gateway device.
Primary/ Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Lease Time	Select **Infinite** to have the binding always valid. Select the second radio button to set up the binding's valid days, hours and minutes.

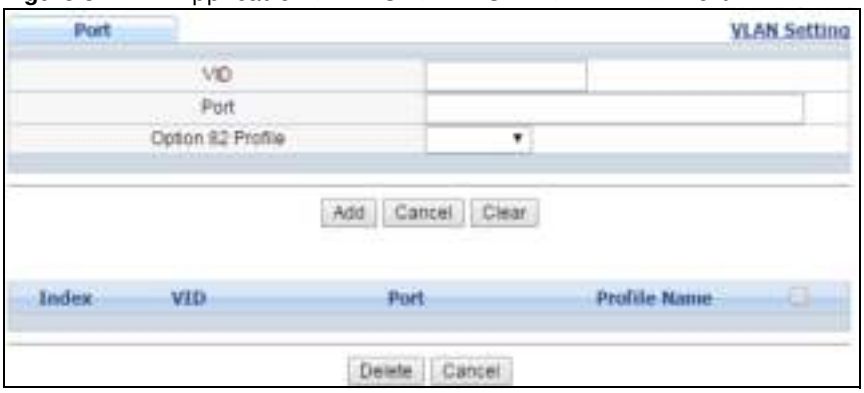
Table 209 IP Application > DHCP > DHCPv4 > VLAN (continued)

LABEL	DESCRIPTION
Relay	Use this section if you want to configure the Switch to function as a DHCP relay for this VLAN.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays **Server** or **Relay** for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the configuration entries you want to remove and click **Delete** to remove them.
Cancel	Click **Cancel** to clear the check boxes.

43.5.1 DHCPv4 VLAN Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. To open this screen, click **IP Application > DHCP > DHCPv4 > VLAN > Port**.

Figure 312 IP Application > DHCP > DHCPv4 > VLAN > Port



The following table describes the labels in this screen.

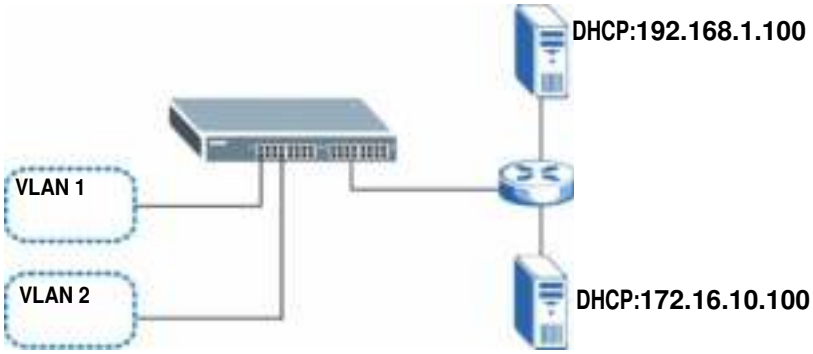
Table 210 IP Application > DHCP > DHCPv4 > VLAN > Port

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s) in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. Note: The profile you select here has priority over the one you select in the **DHCP > DHCPv4 > VLAN** screen.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** 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 above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the port(s) belongs.
Port	This field displays the port(s) to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s) in this VLAN.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the configuration entries you want to remove and click **Delete** to remove them.
Cancel	Click **Cancel** to clear the check boxes.

43.5.2 Example: DHCP Relay for Two VLANs

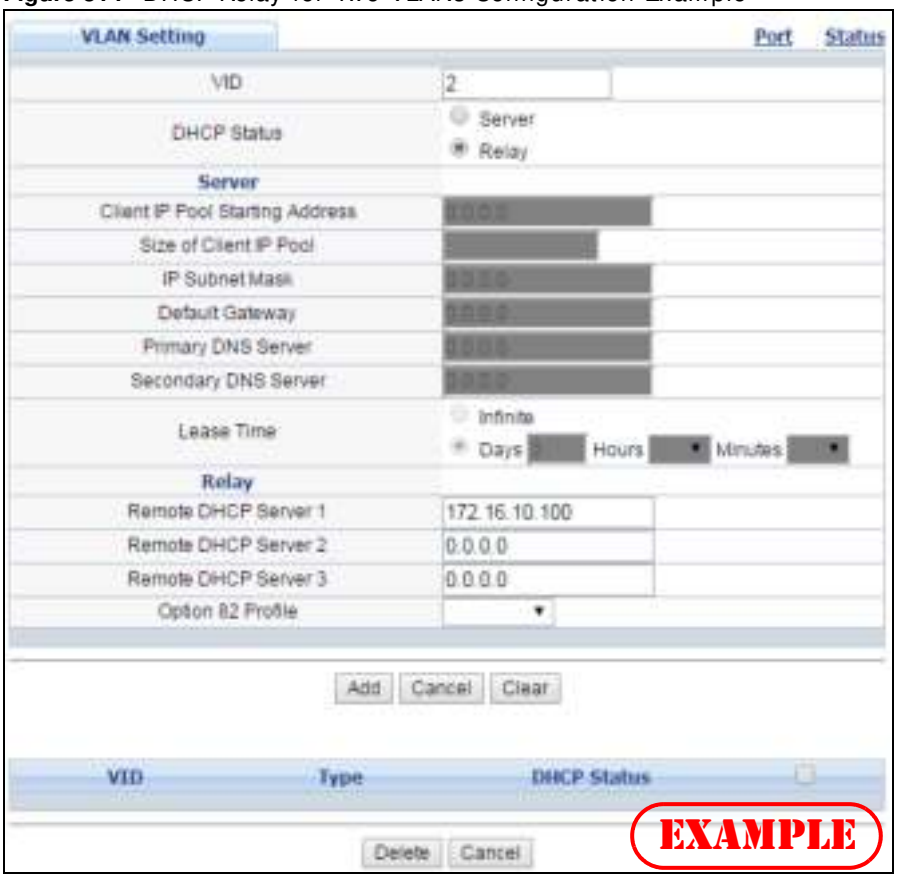
The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.16.10.100.

Figure 313 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

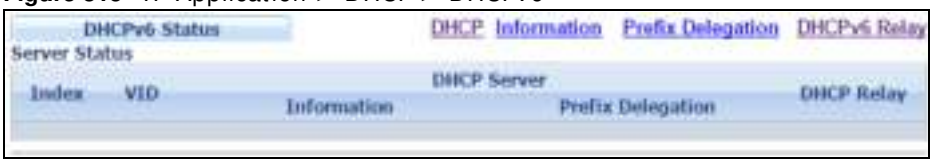
Figure 314 DHCP Relay for Two VLANs Configuration Example



43.6 DHCPv6 Status

Click **IP Application** > **DHCP** > **DHCPv6** in the navigation panel to see information on the DHCPv6 server. The **DHCP Status** screen displays.

Figure 315 IP Application > DHCP > DHCPv6



The following table describes the labels in this screen.

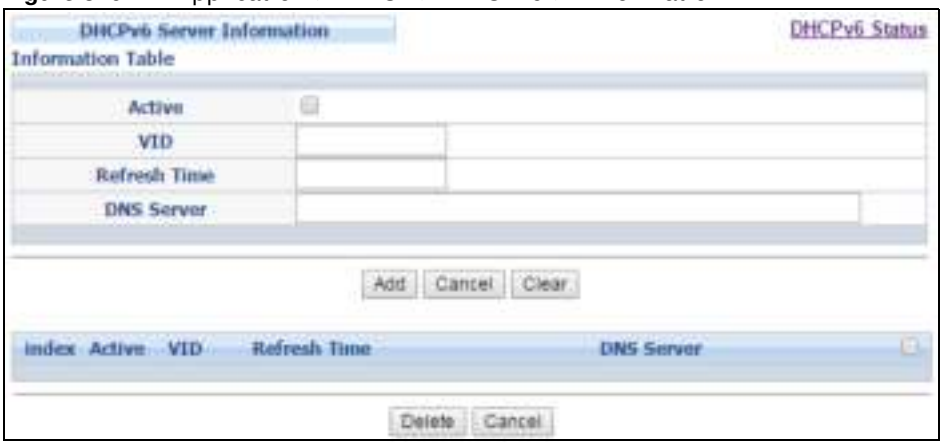
Table 211 IP Application > DHCP > DHCPv6

LABEL	DESCRIPTION
Server Status	This section displays configuration settings related to the Switch's DHCP server mode.
Index	The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.
VID	This is the index number of a DHCPv6 server information
DHCP Server	This field displays the VLAN ID to which the DHCP server belongs.
Information	This field displays **Yes** when the entry supports display of the refresh time and DNS server; it shows **No** when it does not.
Prefix Delegation	This field displays **Yes** when the entry supports the prefix delegation; it shows **No** when it does not. The prefix delegation is used by an IPv6 device to generate its IP address.
DHCP Relay	A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server (that's in another network) and the DHCPv6 clients. This field displays **Yes** when the Switch supports DHCPv6 Relay and **No** when it does not. **Yes** means the Switch forwards all DHCP requests to the same DHCP server. **No** means the Switch does not forward DHCP requests to a DHCP server.

43.7 DHCPv6 Information

Use this screen to configure DHCPv6 and DNS server settings on the Switch. Click **IP Application > DHCP > DHCPv6 > Information** in the navigation panel to display the screen as shown.

Figure 316 IP Application > DHCP > DHCPv6 > Information



The following table describes the labels in this screen.

Table 212 IP Application > DHCP > DHCPv6 > Information

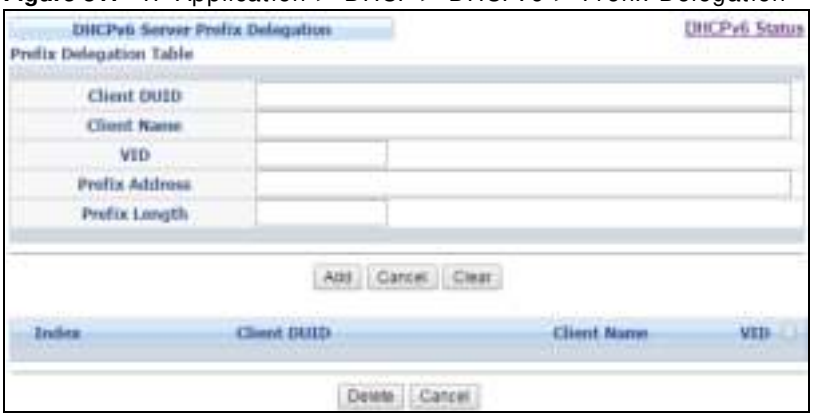
LABEL	DESCRIPTION
Active	Select this check box to enable the Switch to get DHCPv6 and DNS server settings.
VID	Enter the ID number of the VLAN to which the DHCPv6 server belongs here.
Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from a DHCPv6 server. The allowed range is 600 to 4294967295 seconds.
DNS Server	Specify the IPv6 address of the DNS server for the DHCP clients to use here. An 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'.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change its settings.
Active	This field displays whether the DHCPv6 is activated or not.
VID	This field displays the ID number of the VLAN to which the DHCPv6 server belongs.
Refresh Time	This field displays the number of seconds a DHCPv6 client should wait before refreshing information retrieved from a DHCPv6 server. It displays **disable** if **Refresh Time** is not configured.
DNS Server	This field displays the IPv6 address of the DNS server that the DHCP clients will use. It displays **disable** when it is not configured.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

43.8 DHCPv6 Prefix Delegation

Prefix delegation enables an IPv6 device to use the received IPv6 prefix (for example, '2001:db2::/48') to generate its IP address. The Switch passes the the IPv6 prefix information to its connected hosts (according to VLAN) so that they can generate their IPv6 addresses.

Use this screen to configure DHCPv6 client and IPv6 prefix settings for a specific VLAN on the Switch. Click **IP Application > DHCP > DHCPv6 > Prefix Delegation** in the navigation panel to display the screen as shown.

Figure 317 IP Application > DHCP > DHCPv6 > Prefix Delegation



The following table describes the labels in this screen.

Table 213 IP Application > DHCP > DHCPv6 > Prefix Delegation

LABEL	DESCRIPTION
Client DUID	Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. Type the client DUID for the devices connected to the Switch in this field.
Client Name	Type a name to identify the DHCPv6 client in this field.
VID	Type the ID number of the VLAN to which the DHCPv6 client belongs here.
Prefix Address	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' is a prefix address with prefix length. /32 means that the first 32 bits ('2001:db8') from the left is the network prefix. Type the prefix address in this field. For example, type '2001:db8:1a2b:15::1a2f:0'
Prefix Length	Type the prefix length in this field. For example, type 32.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change its settings.
Client DUID	This field displays the client DHCP Unique IDentifier (DUID) which uniquely identifies the client.
Client Name	This field displays a name to identify the DHCPv6 client.
VID	This field displays the ID number of the VLAN to which the DHCPv6 client belongs.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

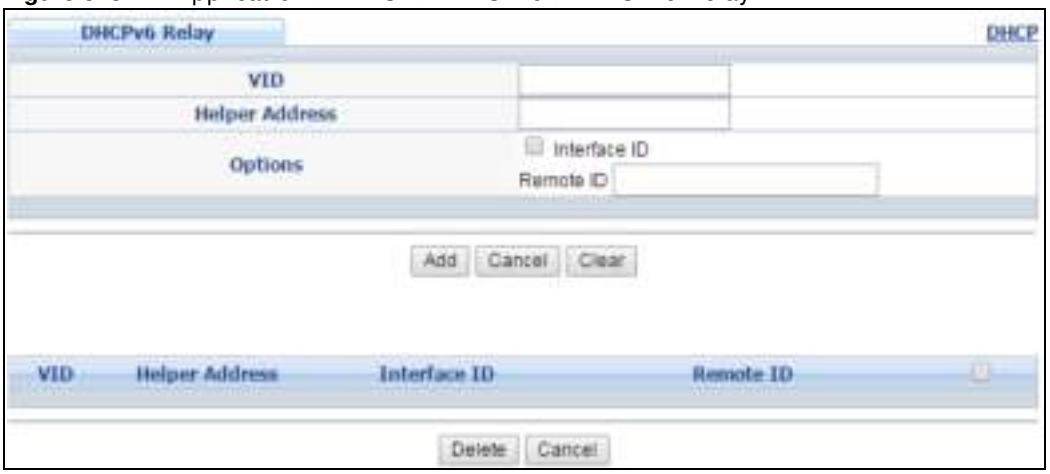
43.9 DHCPv6 Relay

A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server (that's in another network) and the DHCPv6 clients.

The DHCPv6 relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCPv6 server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Use this screen to configure DHCPv6 relay settings for a specific VLAN on the Switch. Click **IP Application > DHCP > DHCPv6 > DHCPv6 Relay** in the navigation panel to display the screen as shown.

Figure 318 IP Application > DHCP > DHCPv6 > DHCPv6 Relay



The following table describes the labels in this screen.

Table 214 IP Application > DHCP > DHCPv6> DHCPv6 Relay

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which the DHCPv6 server that will assign IP information belongs here.
Helper Address	Enter the IPv6 address of the DHCPv6 server that will assign IP information here. An 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'.
Options	

Table 214 IP Application > DHCP > DHCPv6> DHCPv6 Relay (continued)

LABEL	DESCRIPTION
Interface ID	Select this option to have the Switch add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Remote ID	Enter a string of up to 64 printable characters to be carried in the remote-ID option. The Switch adds the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to reset the fields to the factory defaults.
VID	This field displays the VLAN ID number. Click the VLAN ID to change the settings.
Helper Address	This field displays the IPv6 address of the remote DHCPv6 server for this VLAN.
Interface ID	This field displays whether the interface-ID option is added to DHCPv6 requests from clients in this VLAN.
Remote ID	This field displays whether the remote-ID option is added to DHCPv6 requests from clients in this VLAN.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es).

44

VRRP

This chapter shows you how to configure and monitor the Virtual Router Redundancy Protocol (VRRP) on the Switch.

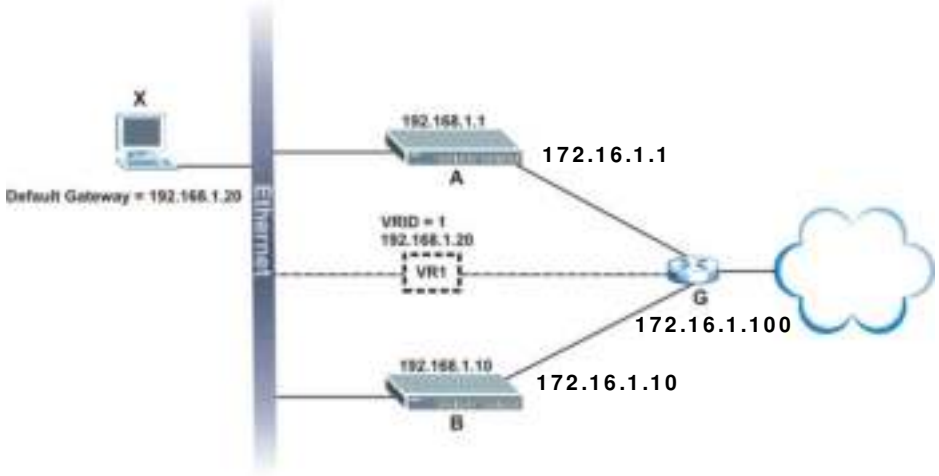
44.1 VRRP Overview

Each host on a network is configured to send packets to a statically configured default gateway (this Switch). The default gateway can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

In VRRP, a virtual router (VR) represents a number of physical layer-3 devices. An IP address is associated with the virtual router. A layer-3 device having the same IP address is the preferred master router while the other Layer-3 devices are the backup routers. The master router forwards traffic for the virtual router. When the master router becomes unavailable, a backup router assumes the role of the master router until the master router comes back up and takes over.

The following figure shows a VRRP network example with the switches (**A** and **B**) implementing one virtual router **VR1** to ensure the link between the host **X** and the uplink gateway **G**. Host **X** is configured to use **VR1** (192.168.1.20) as the default gateway. If switch **A** has a higher priority, it is the master router. Switch **B**, having a lower priority, is the backup router.

Figure 319 VRRP: Example 1



If switch **A** (the master router) is unavailable, switch **B** takes over. Traffic is then processed by switch **B**.

44.2 VRRP Status

Click **IP Application** > **VRRP** in the navigation panel to display the **VRRP Status** screen as shown next.

Figure 320 IP Application > VRRP Status

The following table describes the labels in this screen.

Table 215 IP Application > VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Network	This field displays the IP address and the subnet mask bits of an IP routing domain that is associated to a virtual router.
VRID	This field displays the ID number of the virtual router.
VR Status	This field displays the status of the virtual router. This field is **Master** indicating that this Switch functions as the master router. This field is **Backup** indicating that this Switch functions as a backup router. This field displays **Init** when this Switch is initiating the VRRP protocol or when the **Uplink Status** field displays **Dead**.
Uplink Status	This field displays the status of the link between this Switch and the uplink gateway. This field is **Alive** indicating that the link between this Switch and the uplink gateway is up. Otherwise, this field is **Dead**. This field displays **Probe** when this Switch is check for the link state.
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 **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.

44.3 VRRP Configuration

The following sections describe the different parts of the VRRP Configuration screen.

44.3.1 IP Interface Setup

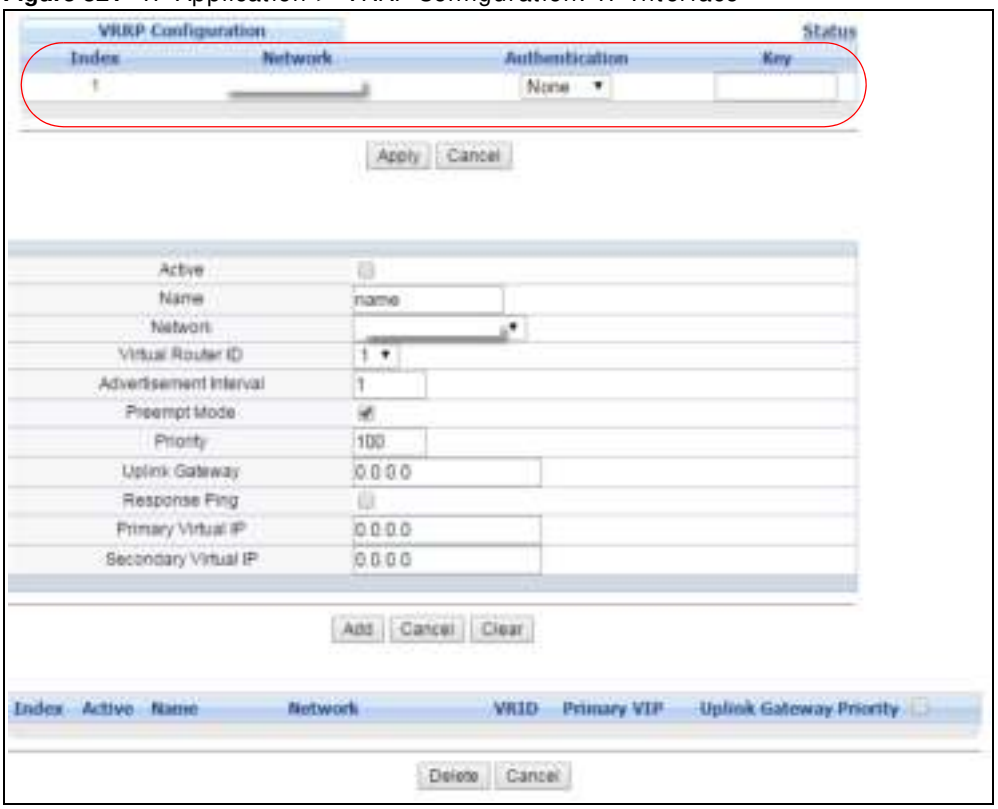
Before configuring VRRP, first create an IP interface (or routing domain) in the **IP Setup** screen (see the Section 6.5 on page 65 for more information).

Click **IP Application**, **VRRP** and click the **Configuration** link to display the **VRRP Configuration** screen as shown next.

Note: You can only configure VRRP on interfaces with unique VLAN IDs.

Note: Routing domains with the same VLAN ID are not displayed in the table indicated.

Figure 321 IP Application > VRRP Configuration: IP Interface



The following table describes the labels in this screen.

Table 216 IP Application > VRRP Configuration: IP Interface

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Network	This field displays the IP address and number of subnet mask bit of an IP domain.
Authentication	Select **None** to disable authentication. This is the default setting. Select **Simple** to use a simple password to authenticate VRRP packet exchanges on this interface.
Key	When you select **Simple** in the **Authentication** field, enter a password key (up to eight printable ASCII character long) in this field.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to discard all changes made in this table.

44.3.2 VRRP Parameters

This section describes the VRRP parameters.

44.3.2.1 Advertisement Interval

The master router sends out Hello messages to let the other backup routers know that it is still up and running. The time interval between sending the Hello messages is the advertisement interval. By default, a Hello message is sent out every second.

If the backup routers do not receive a Hello message from the master router after this interval expires, it is assumed that the master router is down. Then the backup router with the highest priority becomes the master router.

Note: All routers participating in the virtual router must use the same advertisement interval.

44.3.2.2 Priority

Configure the priority level (1 to 254) to set which backup router to take over in case the master router goes down. The backup router with the highest priority will take over. The priority of the VRRP router that owns the IP address(es) associated with the virtual router is 255.

44.3.2.3 Preempt Mode

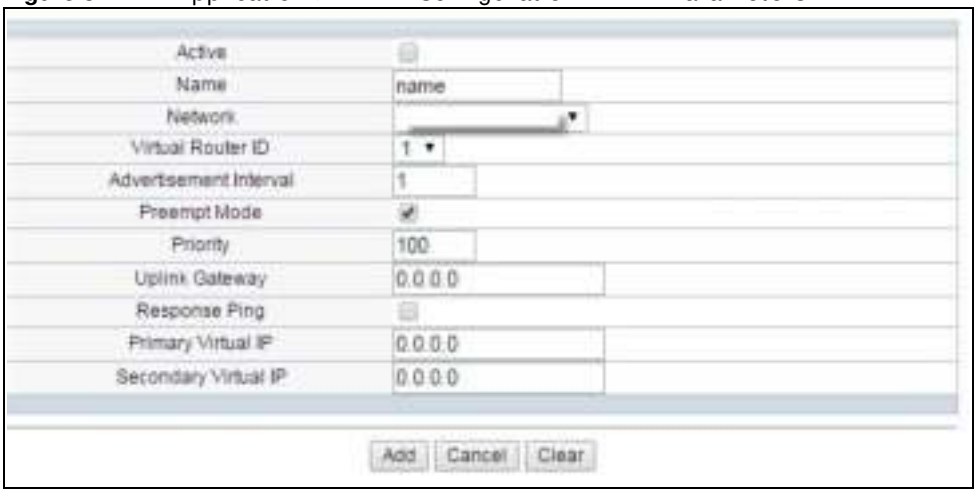
If the master router is unavailable, a backup router assumes the role of the master router. However, when another backup router with a higher priority joins the network, it will preempt the lower priority backup router that is the master. Disable preempt mode to prevent this from happening.

By default, a layer 3 device with the same IP address as the virtual router will become the master router regardless of the preempt mode.

44.3.3 Configuring VRRP Parameters

After you set up an IP interface, configure the VRRP parameters in the **VRRP Configuration** screen.

Figure 322 IP Application > VRRP Configuration: VRRP Parameters



The following table describes the labels in this screen.

Table 217 IP Application > VRRP Configuration: VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Network	Select an IP domain to which this VRRP entry applies.
Virtual Router ID	Select a virtual router number (1 to 7) for which this VRRP entry is created. You can configure up to seven virtual routers for one network.
Advertisement Interval	Specify the number of seconds between Hello message transmissions. The default is **1**.
Preempt Mode	Select this option to activate preempt mode.
Priority	Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority. This field is **100** by default.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The Switch checks the link to the uplink gateway.
Response Ping	Select this option to have the Switch respond to a ping that is sent to the virtual IP address.
Primary Virtual IP	Enter the IP address of the primary virtual router in dotted decimal notation.
Secondary Virtual IP	This field is optional. Enter the IP address of a secondary virtual router in dotted decimal notation. This field is ignored when you enter **0.0.0.0**.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to discard all changes made in this table.
Clear	Click **Clear** to set the above fields back to the factory defaults.

44.3.4 Viewing VRRP Summary

View the VRRP configuration summary at the bottom of the screen.

Figure 323 IP Application > VRRP Configuration: Summary

The following table describes the labels in this screen.

Table 218 IP Application > VRRP Configuration: Summary

LABEL	DESCRIPTION
Index	This field displays the index number of an entry. Click an index number to change the settings.
Active	This field shows whether a VRRP entry is enabled (**Yes**) or disabled (**No**).

Table 218 IP Application > VRRP Configuration: Summary (continued)

LABEL	DESCRIPTION
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and subnet mask of an interface.
VRID	This field displays the ID number of a virtual router.
Primary VIP	This field displays the IP address of the primary virtual router.
Uplink Gateway	This field displays the IP address of the uplink gateway.
Priority	This field displays the priority level (1 to 255) of the entry.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

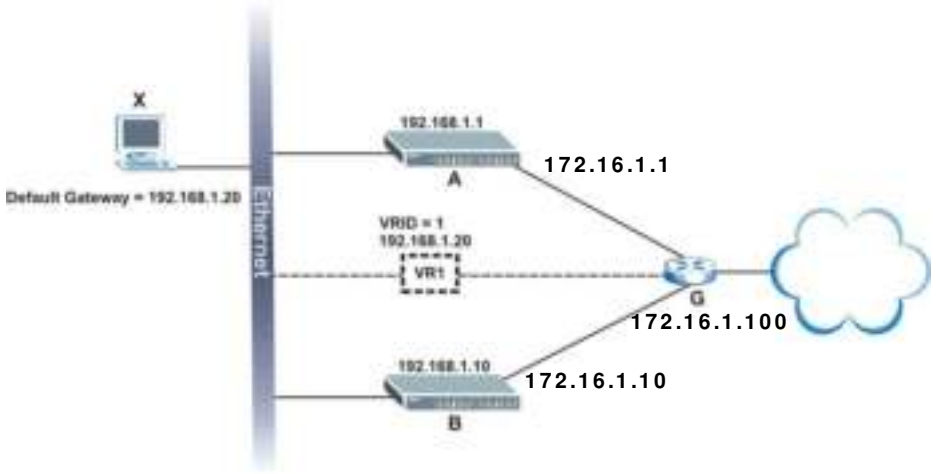
44.4 VRRP Configuration Examples

The following sections show two VRRP configuration examples on the Switch.

44.4.1 One Subnet Network Example

The figure below shows a simple VRRP network with only one virtual router **VR1** (VRID = 1) and two switches. The network is connected to the WAN via an uplink gateway **G** (172.16.1.100). The host computer **X** is set to use **VR1** as the default gateway.

Figure 324 VRRP Configuration Example: One Virtual Router Network



You want to set switch **A** as the master router. Configure the VRRP parameters in the **VRRP Configuration** screens on the switches as shown in the figures below.

Figure 325 VRRP Example 1: VRRP Parameter Settings on Switch A

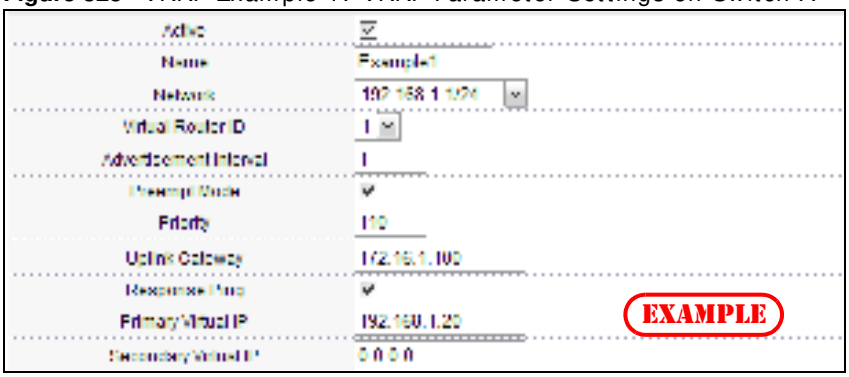
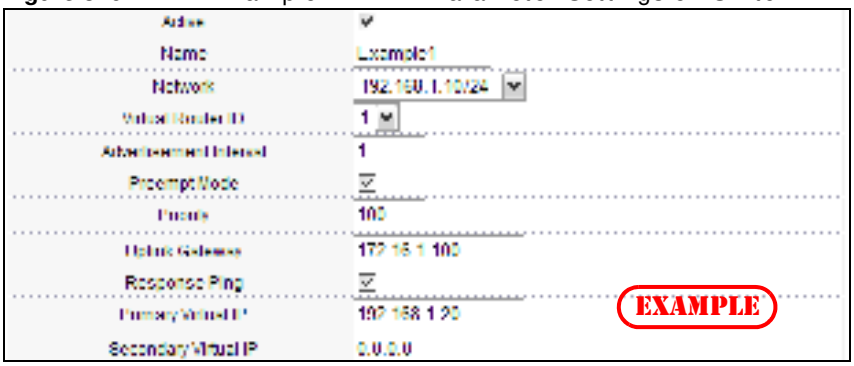


Figure 326 VRRP Example 1: VRRP Parameter Settings on Switch B



After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 327 VRRP Example 1: VRRP Status on Switch A

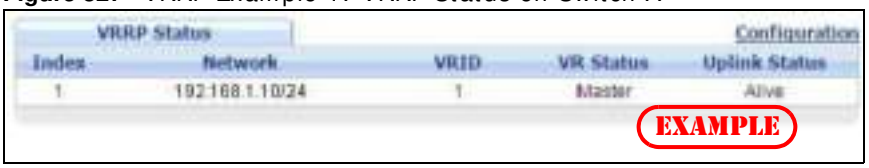
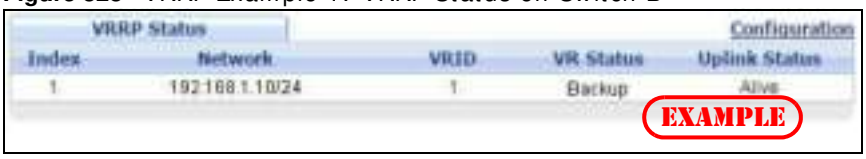


Figure 328 VRRP Example 1: VRRP Status on Switch B

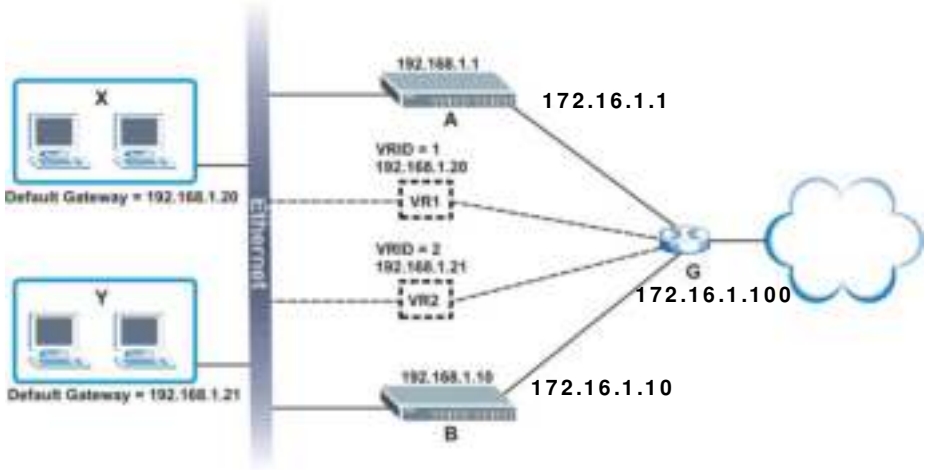


44.4.2 Two Subnets Example

The following figure depicts an example in which two switches share the network traffic. Hosts in the two network groups use different default gateways. Each switch is configured to backup a virtual router using VRRP.

You wish to configure switch **A** as the master router for virtual router **VR1** and as a backup for virtual router **VR2**. On the other hand, switch **B** is the master for **VR2** and a backup for **VR1**.

Figure 329 VRRP Configuration Example: Two Virtual Router Network



You need to configure the **VRRP Configuration** screen for virtual router VR2 on each switch, while keeping the VRRP configuration in example 1 for virtual router **VR1** (refer to Section 44.4.2 on page 436). Configure the VRRP parameters on the switches as shown in the figures below.

Figure 330 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A

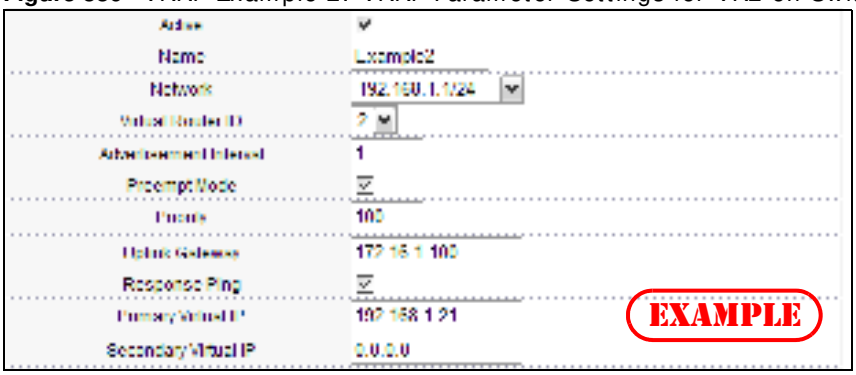
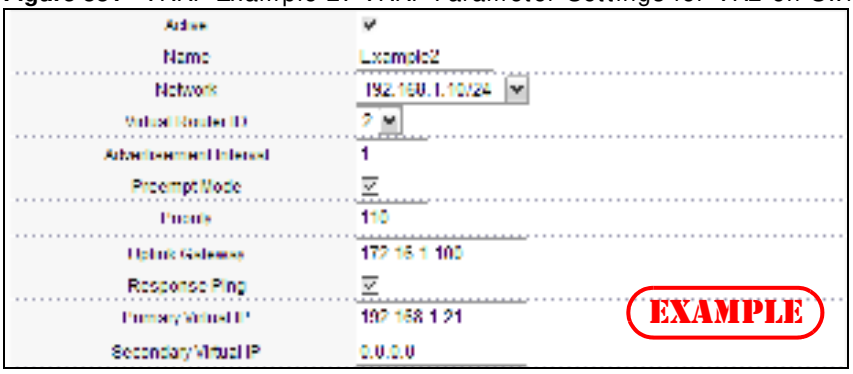


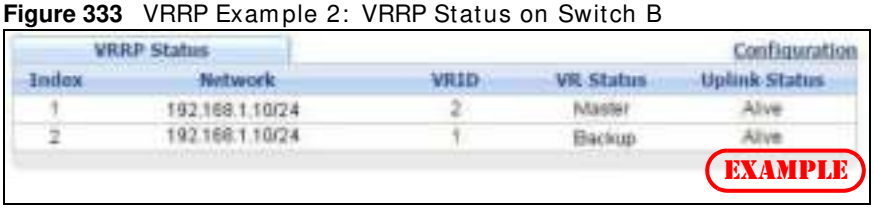
Figure 331 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B



After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 332 VRRP Example 2: VRRP Status on Switch A

Figure 333 VRRP Example 2: VRRP Status on Switch B

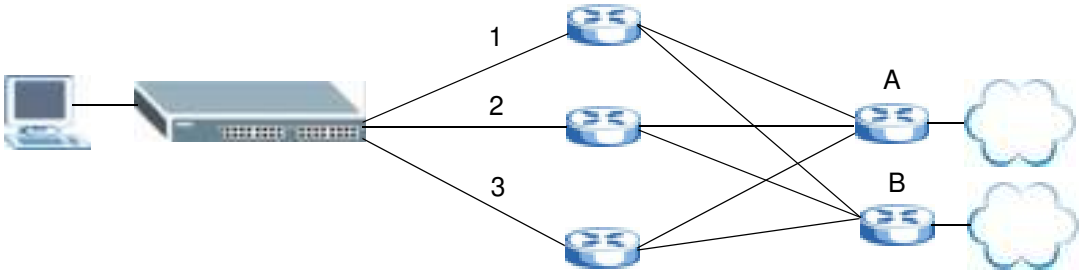


45

Load Sharing

45.1 Load Sharing Overview

The Switch learns the next-hop(s) using ARP and determines routing path(s) for a destination. The Switch supports Equal-Cost MultiPath (ECMP) to forward packets destined to the same device (**A** for example) through different routing paths (**1**, **2** and **3**) of equal path cost. This allows you to balance or share traffic loads between multiple routing paths when the Switch is connected to more than one next-hop. ECMP works with static routes or a routing protocol, such as OSPF.

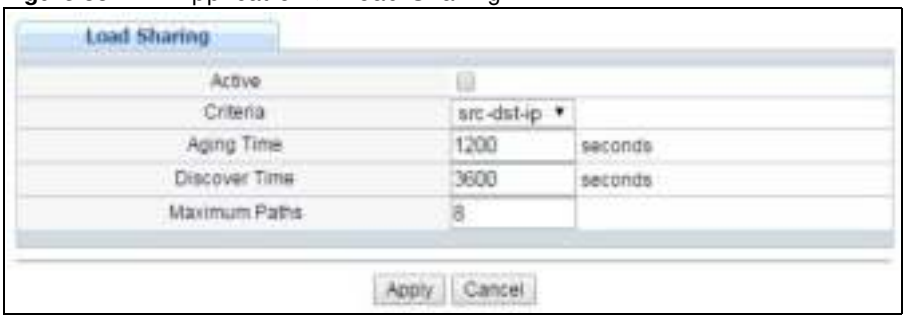


With ECMP, packets are routed through the paths of equal cost according to the hash algorithm output.

45.2 Configuring Load Sharing

Click **IP Application** > **Load Sharing** in the navigation panel to display the screen as shown next.

Figure 334 IP Application > Load Sharing



The following table describes the labels in this screen.

Table 219 IP Application > Load Sharing

LABEL	DESCRIPTION
Active	Select this option to enable Equal-Cost MultiPath (ECMP) routing on the Switch.
Criteria	Select the criteria the Switch uses to determine the routing path for a packet. Select **src-ip** to have the Switch use a hash algorithm to convert a packet's source IP address into a hash value which acts as an index to a route path. Select **src-dst-ip** to have the Switch use a hash algorithm to convert a packet's source and destination IP addresses into a hash value which acts as an index to a route path.
Aging Time	Specify the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update a resolved next-hop's MAC address.
Discover Time	Specify the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update an unresolved next-hop's MAC address.
Maximum Paths	Set the maximum number of paths for one ECMP (Equal-Cost MultiPath) route. The maximum number varies by Switch. A smaller number of maximum-paths means more ECMP routes are allowed and a larger number of maximum-paths means fewer ECMP routes are allowed. The number of paths for a static route for ECMP cannot be bigger than the maximum-paths value configured here. Throughput may be influenced while configuring ECMP maximum-paths.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

46

ARP Setup

46.1 ARP 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.

46.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch looks in the ARP Table and if it finds the address, it 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.

46.1.2 ARP Learning Mode

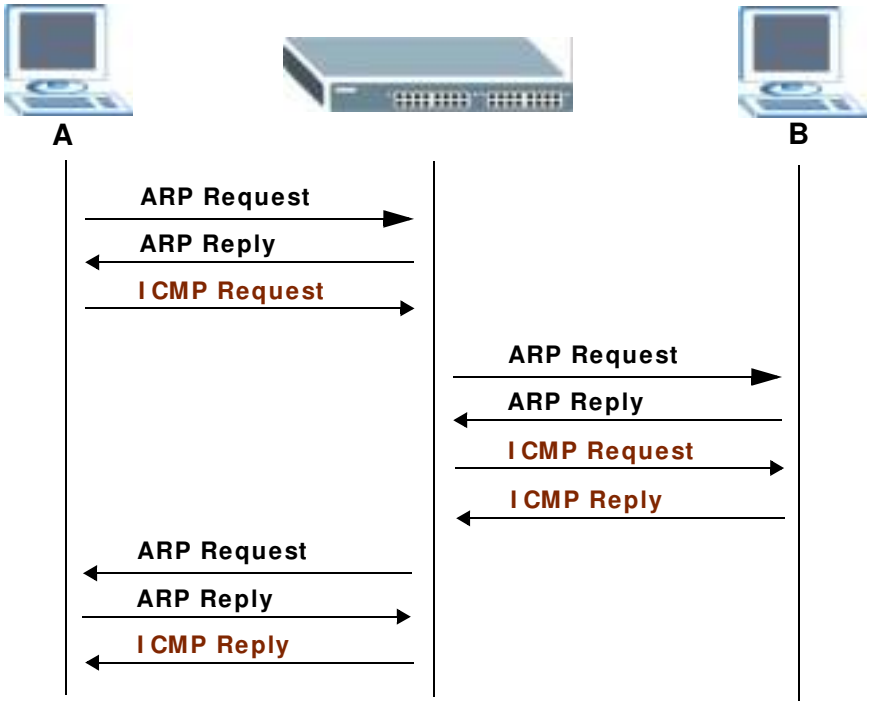
The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

46.1.2.1 ARP-Reply

The Switch in ARP-Reply learning mode updates the ARP table only with the ARP replies to the ARP requests sent by the Switch. This can help prevent ARP spoofing.

In the following example, the Switch does not have IP address and MAC address mapping information for hosts **A** and **B** in its ARP table, and host **A** wants to ping host **B**. Host **A** sends an ARP request to the Switch and then sends an ICMP request after getting the ARP reply from the Switch. The Switch finds no matched entry for host **B** in the ARP table and broadcasts the ARP request to all the devices on the LAN. When the Switch receives the ARP reply from host **B**, it updates its ARP table and also forwards host **A**'s ICMP request to host **B**. After the Switch gets the

ICMP reply from host **B**, it sends out an ARP request to get host **A**'s MAC address and updates the ARP table with host **A**'s ARP reply. The Switch then can forward host **B**'s ICMP reply to host **A**.



46.1.2.2 Gratuitous-ARP

A gratuitous ARP is an ARP request in which both the source and destination IP address fields are set to the IP address of the device that sends this request and the destination MAC address field is set to the broadcast address. There will be no reply to a gratuitous ARP request.

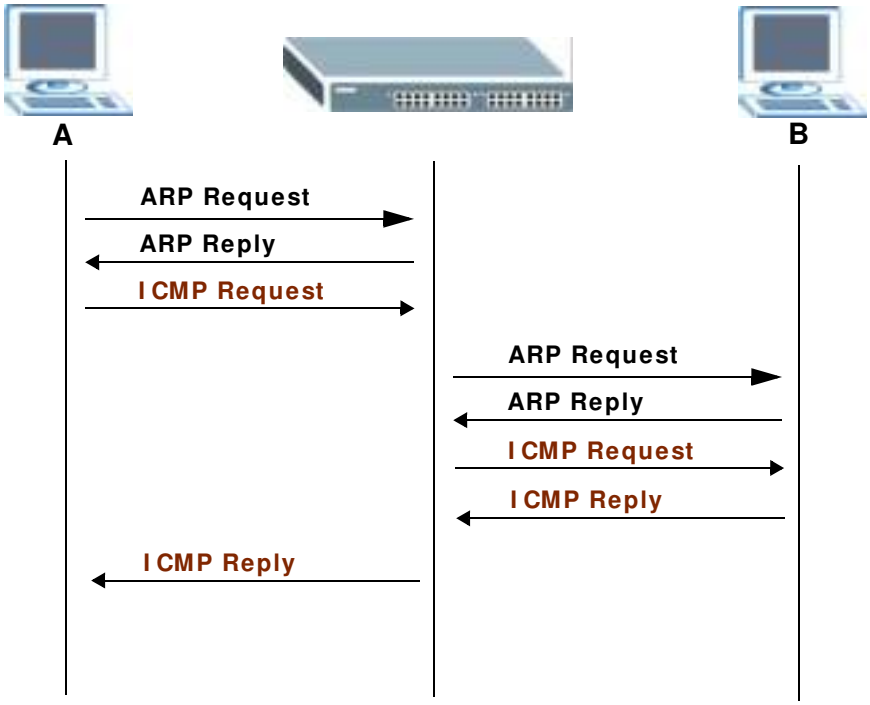
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

46.1.2.3 ARP-Request

When the Switch is in ARP-Request learning mode, it updates the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.

Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



46.2 ARP Setup

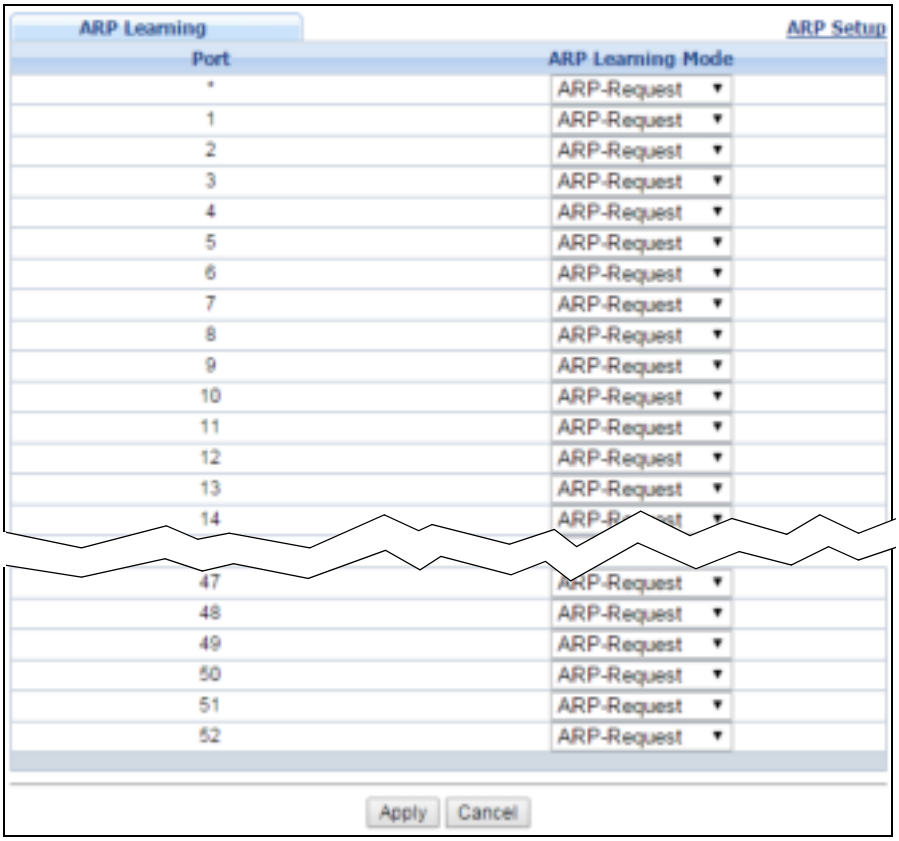
Click **IP Application** > **ARP Setup** in the navigation panel to display the screen as shown. Click the link next to **ARP Learning** to open a screen where you can set the ARP learning mode for each port. Click the link next to **Static ARP** to open a screen where you can create static ARP entries on the Switch.

Figure 335 IP Application > ARP Setup

46.2.1 ARP Learning

Use this screen to configure each port's ARP learning mode. Click the link next to **ARP Learning** in the **IP Application** > **ARP Setup** screen to display the screen as shown next.

Figure 336 IP Application > ARP Setup > ARP Learning



The following table describes the labels in this screen.

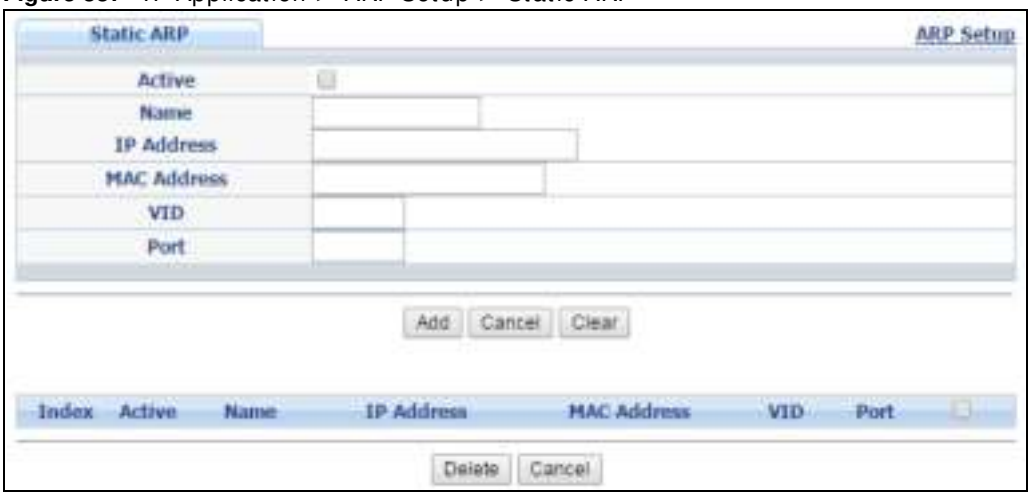
Table 220 IP Application > ARP Setup > ARP Learning

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This field displays the port number. In stacking mode, the first number represents the slot and the second 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.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select **ARP-Reply** to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select **Gratuitous-ARP** to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select **ARP-Request** to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

46.2.2 Static ARP

Use this screen to create static ARP entries that will display in the **Management > ARP Table** screen and will not age out. Click the link next to **Static ARP** in the **IP Application > ARP Setup** screen to display the screen as shown.

Figure 337 IP Application > ARP Setup > Static ARP



The following table describes the related labels in this screen.

Table 221 IP Application > ARP Setup > Static ARP

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 (up to 32 printable ASCII characters) for identification purposes.
IP Address	Enter the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	Enter the MAC address of the device with the corresponding IP address above.
VID	Enter the ID number of VLAN to which the device belongs.
Port	Enter the number of port to which the device connects. In stacking mode, the first number represents the slot and the second the port number.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of an entry. Click an index number to change the settings.
Active	This field displays **Yes** when the entry is activated and **NO** when it is deactivated.
Name	This field displays the descriptive name for this entry. This is for identification purposes only.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.

Table 221 IP Application > ARP Setup > Static ARP (continued)

LABEL	DESCRIPTION
Port	This field displays the port to which the device connects.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

47

Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

47.1 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 338 Management > Maintenance

The following table describes the labels in this screen.

Table 222 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (**Configuration 1** or **Configuration 2**) is currently operating on the Switch.
Firmware Upgrade	Click **Click Here** to go to the **Firmware Upgrade** screen.
Restore Configuration	Click **Click Here** to go to the **Restore Configuration** screen.
Backup Configuration	Click **Click Here** to go to the **Backup Configuration** screen.
Erase Running-Configuration	Click **Click Here** to reset the current configuration of the Switch. Note that this will not reset the configuration to the factory default settings.
Save Configuration	Click **Config 1** to save the current configuration settings to **Configuration 1** on the Switch. Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Table 222 Management > Maintenance (continued)

LABEL	DESCRIPTION
Reboot System	Click **Config 1** to reboot the system and load **Configuration 1** on the Switch. Click **Config 2** to reboot the system and load **Configuration 2** on the Switch. Click **Stacking Default** to reboot the system and load stacking configurations on the Switch. Click **Factory Default** to reboot the system and load the factory default configuration on the Switch. Note: Make sure to click the **Save** button in any screen to save your settings to the current configuration on the Switch.
Tech-Support	Click **Click Here** to see the **Tech-Support** screen. You can set CPU and memory thresholds for log reports and download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.

47.2 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the web configurator and to specify which image is loaded when the Switch starts up.

Click **Management** > **Maintenance** > **Firmware Upgrade** to view the screen as shown next.

Figure 339 Management > Maintenance > Firmware Upgrade (Standalone mode)

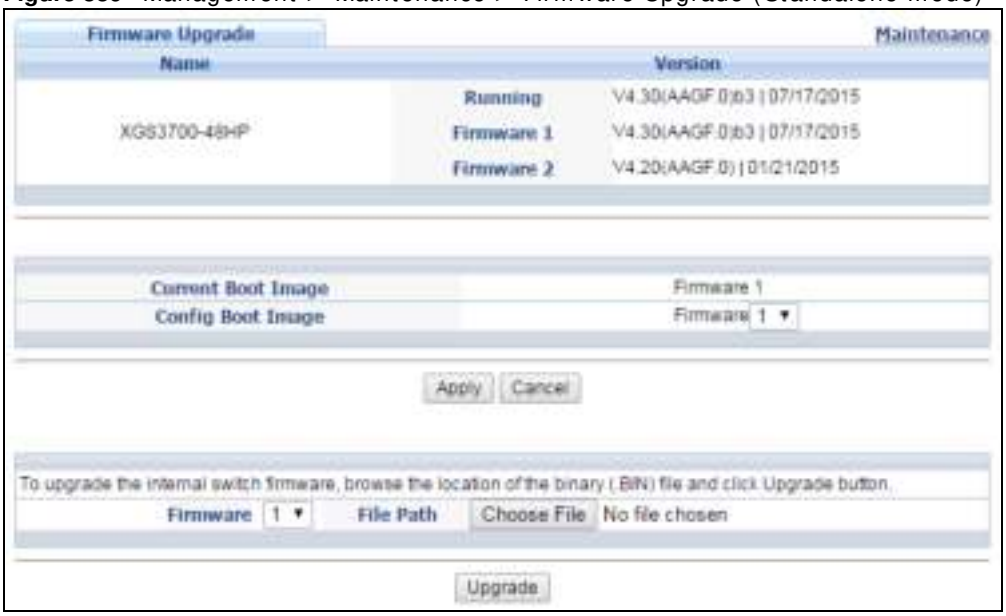
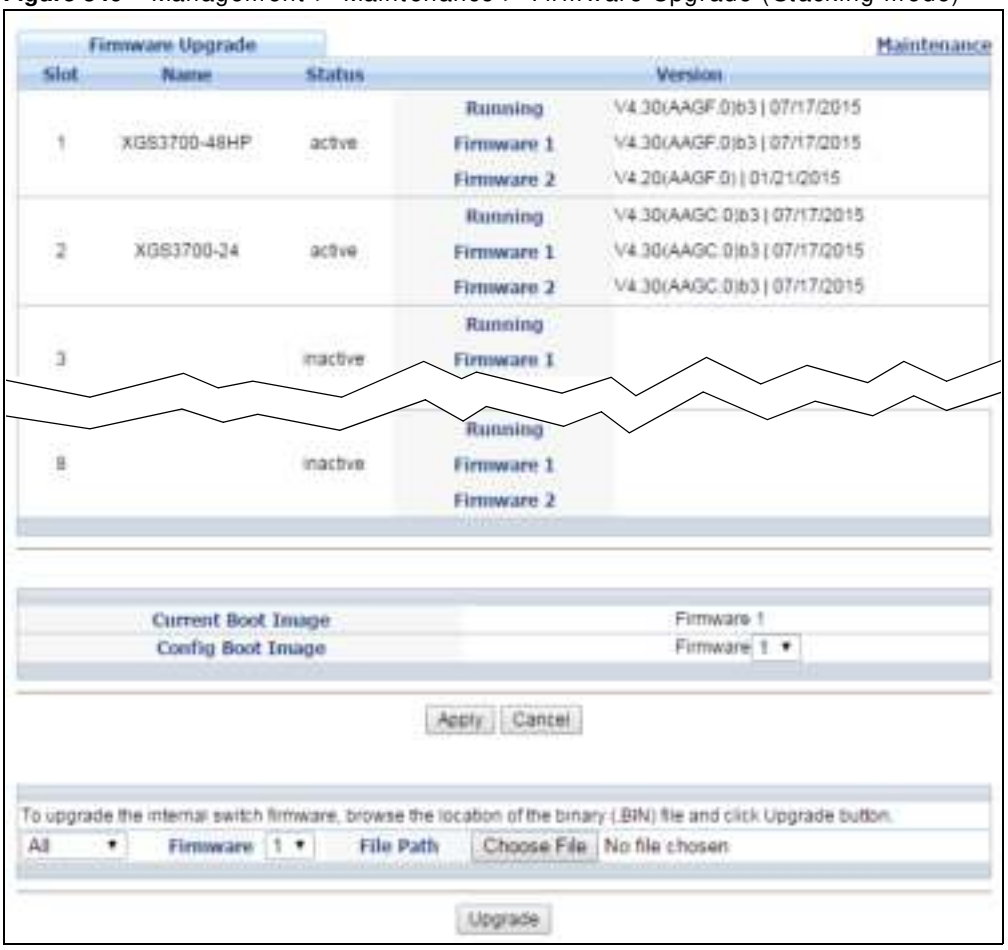


Figure 340 Management > Maintenance > Firmware Upgrade (Stacking mode)



The top of firmware upgrade screen shows which firmware version is currently running on the Switch. 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. Firmware upgrades are only applied after a reboot. Click **Upgrade** to load the new firmware. Select the **Config Boot Image** drop-down list box if you want to reboot the Switch and click **Apply** to apply the new firmware immediately. 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.

Table 223 Management > Maintenance> Firmware Upgrade

LABEL	DESCRIPTION
Slot (Stacking mode)	This is the slot index number.
Name	This is the name of the Switch that you're configuring.
Status (Stacking mode)	This field displays the current stacking status on the Switch.

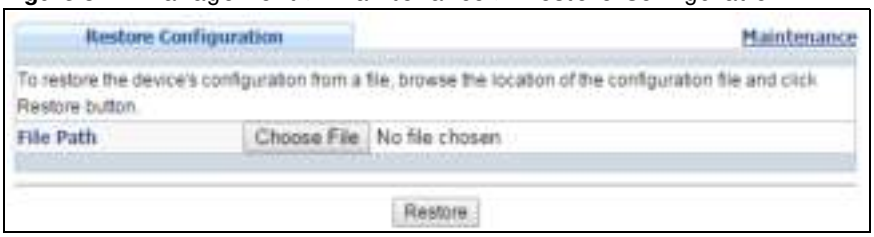
Table 223 Management > Maintenance> Firmware Upgrade (continued)

LABEL	DESCRIPTION
Version	The Switch has two firmware sets, **Firmware 1** and **Firmware 2**, residing in flash. • **Running** shows the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch (**Firmware 1** or **Firmware 2)**. The firmware information is also displayed at System Information in Basic Settings. • **Firmware 1** shows its version number (and model code) and MM/DD/YYYY creation date. • **Firmware 2** shows its version number (and model code) and MM/DD/YYYY creation date.
Current Boot Image	This displays which firmware is currently in use on the Switch (**Firmware 1** or **Firmware 2)**.
Config Boot Image	Select which firmware (**Firmware 1** or **Firmware 2)** should load after rebooting. Click Apply and reboot the Switch to see changes including in the **Current Boot Image** field.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
(Stacking mode)	Click the drop-down list to choose the slot number of the Switch in a stack to upgrade the firmware on this slot. Or select **All** to upgrade the firmware for all slots.
Firmware	Choose to upload the new firmware to (Firmware) **1** or (Firmware) **2**.
Choose File	Click this and locate the path and file name of the firmware file you wish to upload to the Switch.
Upgrade	Click **Upgrade** to load the new firmware. Firmware upgrades are only applied after a reboot. To reboot, go to **Management > Maintenance > Reboot System**. You may also click **Config 1**, **Config 2**, or **Factory Default** (**Config 1**, **Config 2** and **Factory Default** are the configuration files you want the Switch to use when it restarts).

47.3 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 341 Management > Maintenance > Restore Configuration



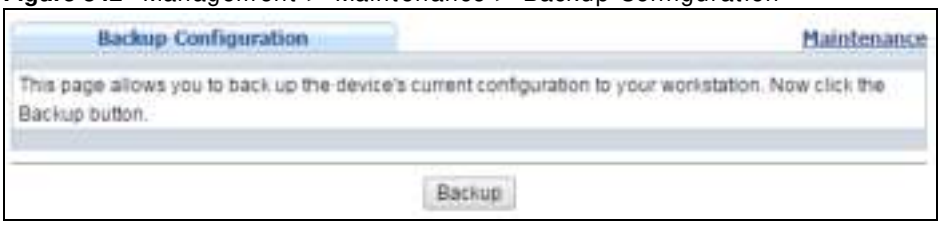
Click the **Choose File** button to upload the path and file name of the configuration file you wish to restore in the **File Path** text box. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

47.4 Backup a Configuration File

Backing up your Switch configurations allows you to create various “snapshots” 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 342 Management > Maintenance > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Click **Backup**.

2 If the current configuration file is open and/or downloaded to your computer automatically, you can click **File > Save** As to save the file to a specific place.

If a dialog box pops up asking whether you want to open or save the file, click **Save** or **Save File** to download it to the default downloads folder on your computer. If a **Save As** screen displays after you click **Save** or **Save File**, Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

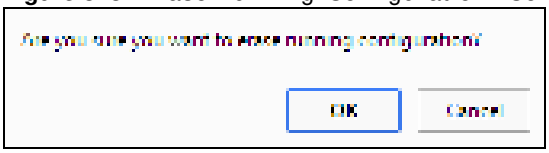
47.5 Erase Running-Configuration

Follow the steps below to clear current configuration on the Switch. Note that this will NOT reset the Switch back to its factory defaults. For example, if your Switch is set to stacking mode and you click erase running-configuration, after the the Switch restarts, it will remain in stacking mode. If you want to change the Switch to its factory default mode, click Factory Default button in Reboot System. See (Section 47.7.1 on page 452).

1 In the **Maintenance** screen, click the **Click Here** button next to **Erase Running-Configuration** to clear all Switch configuration information you configured on the Switch..

2 Click **OK** to reset all Switch configurations.

Figure 343 Erase Running-Configuration: Confirmation



3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you 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).

47.6 Save Configuration

Click **Config 1** to save the current configuration settings permanently to configuration one on the Switch.

Click **Config 2** to save the current configuration settings permanently to configuration two 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.

47.7 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**),configuration two (**Config 2**), stacking default, or factory default 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 344 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.

Click **Factory Default** and follow steps 1 to 2 to reboot and load default configuration settings on the Switch.

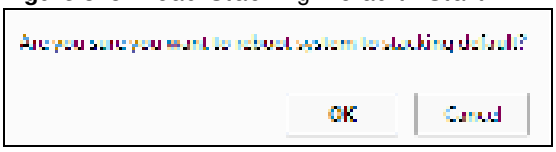
47.7.1 Load Stacking Default

Follow the steps below to reset the Switch back to the stacking defaults. The master Switch login information will not be reset.

1 In the click the **Stacking Default** button to clear all Switch configuration information you configured and return to the stacking defaults.

2 Click **OK** to reset all Switch configurations to the stacking defaults.

Figure 345 Load Stacking Default: Start



3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you 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).

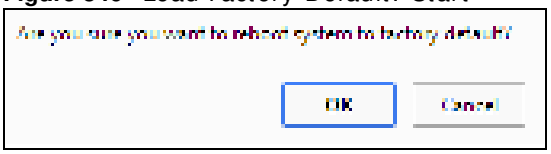
47.7.2 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

1 In the click the **Factory Default** button to clear all Switch configuration information you configured and return to the factory defaults.

2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 346 Load Factory Default: Start



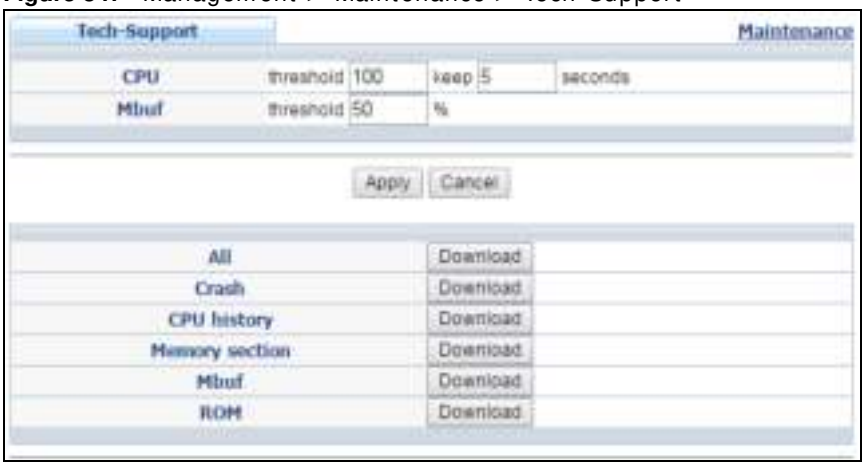
3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

47.8 Tech-Support

The Tech-Support feature is a log enhancement tool that logs useful information such as CPU utilization history, memory and Mbuf (Memory Buffer) log and crash reports for issue analysis by customer support should you have difficulty with your Switch. The Tech Support menu eases your effort in obtaining reports and it is also available in CLI command by typing “Show tech-support” command.

Click **Menu** > **Management** > **Maintenance** > **Tech-Support** to see the following screen.

Figure 347 Management > Maintenance > Tech-Support



You may need WordPad or similar software to see the log report correctly. The table below describes the fields in the above screen.

Table 224 Management > Maintenance > Tech-Support

LABEL	DESCRIPTION
CPU	Type a number ranging from 50 to 100 in the CPU threshold box, and type another number ranging from 5 to 60 in the seconds box then click **Apply**. For example, 80 for CPU threshold and 5 for seconds means a log will be created when CPU utilization reaches over 80% and lasts for 5 seconds. The log report holds 7 days of CPU log data and is stored in volatile memory (RAM). The data is lost if the Switch is turned off or in event of power outage. After 7 days, the logs wrap around and new ones replace the earliest ones. The higher the CPU threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Mbuf	Type a number ranging from 50 to 100 in the Mbuf (Memory Buffer) threshold box. The Mbuf log report is stored in flash (permanent) memory. For example, Mbuf 50 means a log will be created when the Mbuf utilization is over 50%. The higher the Mbuf threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
All	Click **Download** to see all the log report and system status. This log report is stored in flash memory. If the **All** log report is too large, you can download the log reports separately below.
Crash	Click **Download** to see the crash log report. The log will include information of the last crash and is stored in flash memory.
CPU history	Click **Download** to see the CPU history log report. The 7-days log is stored in RAM and you will need to save it, otherwise it will be lost in event of Switch shutdown or power outage.
Memory Section	Click **Download** to see the memory section log report. This log report is stored in flash memory.

Table 224 Management > Maintenance > Tech-Support

LABEL	DESCRIPTION
Mbuf	Click **Download** to see the Mbuf log report. The log includes Mbuf over threshold information. This log report is stored in flash memory.
ROM	Click **Download** to see the Read Only Memory (ROM) log report. This report is stored in flash memory.

47.9 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.

47.9.1 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 225 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	.cfg	This is the configuration (config) 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.

47.9.1.1 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 both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

47.9.2 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 (the default is “admin”).
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 225 on page 455 for more information on filename conventions.
7. Enter `quit` to exit the ftp prompt.

47.9.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 226 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).

47.9.4 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.

48

Access Control

This chapter describes how to control access to the Switch.

48.1 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 usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 227 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 Ethernet Switch CLI Reference Guide for more information on disabling multi-login.

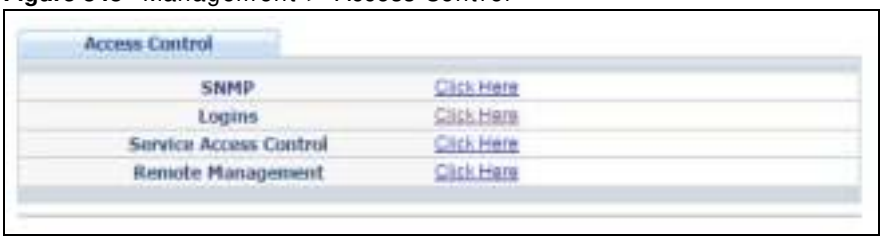
48.1.1 What You Can Do

- Use the **Access Control** screen (Section 48.2 on page 458) to display the main screen.
- Use the **SNMP** screen (Section 48.3.4 on page 465) to configure your SNMP settings.
- Use the **Trap Group** screen (Section 48.3.5 on page 466) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **User Information** screen (Section 48.3.7 on page 469) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **Logins** screens (Section 48.4 on page 471) to assign which users can access the Switch via web configurator at any one time.
- Use the **Service Access Control** screen (Section 48.10 on page 479) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen (Section 48.11 on page 480) to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

48.2 The Access Control Main Screen

Use this screen to display the main screen. Click **Management > Access Control** in the navigation panel to display the main screen as shown.

Figure 348 Management > Access Control



The following table describes the labels in this screen.

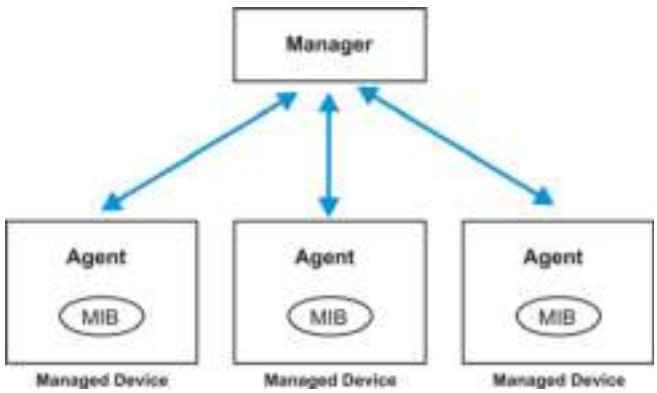
Table 228 Management > Access Control

LABEL	DESCRIPTION
SNMP	Click this link to configure your SNMP settings.
Logins	Click this link to assign which users can access the Switch via web configurator at any one time.
Service Access Control	Click this link to decide what services you may use to access the Switch.
Remote Management	Click this link to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

48.3 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 1 (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 349 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 229 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.

48.3.1 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.

48.3.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- 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

48.3.3 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 "**1.3.6.1.4.1.890.1.15**" is defined in private MIBs. Otherwise, it is a standard MIB OID.

Table 230 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.
fanspeed	zyHwMonitorFanSpeedOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
poe (For PoE models only)	zyPoePowerPortOverload	1.3.6.1.4.1.890.1.15.3.59.4.1	This trap is sent when the port is turned off to supply power due to overloading.
	zyPoePowerPortShortCircuit	1.3.6.1.4.1.890.1.15.3.59.4.2	This trap is sent when the port is turned off to supply power due to short circuit.
	zyPoePowerPortOverSystemBudget	1.3.6.1.4.1.890.1.15.3.59.4.3	This trap is sent when the port is turned off to supply power because the requested power exceeds the total PoE power budget on the Switch.
temperature	zyHwMonitorTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.2	This trap is sent when the temperature goes above or below the normal operating range.
voltage	zyHwMonitorPowerSupplyVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.3	This trap is sent when the voltage goes above or below the normal operating range.
reset	zySysMgmtUncontrolledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.1	This trap is sent when the Switch automatically resets.
	zySysMgmtControlledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.2	This trap is sent when the Switch resets by an administrator through a management interface.
	zySysMgmtBootImageInconsistence	1.3.6.1.4.1.890.1.15.3.49.2.3	This trap is sent when the index number of image which is loaded when the Switch starts up is different from what is specified via the CLI.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.
timesync	zyDateTimeTrapTimeServerNotReachable	1.3.6.1.4.1.890.1.15.3.82.3.1	This trap is sent when the Switch's date and time is not manually entered or the specified time server is not reachable.
intrusionlock	zyPortIntrusionLock	1.3.6.1.4.1.890.1.15.3.61.3.2	This trap is sent when intrusion lock occurs on a port.
loopguard	zyLoopGuardLoopDetect	1.3.6.1.4.1.890.1.15.3.45.2.1	This trap is sent when loopguard shuts down a port.

Table 230 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
errdisable	zyErrdisableDetect	1.3.6.1.4.1.890.1.15.3.24.4.1	This trap is sent when an error is detected on a port, such as a loop occurs or the rate limit for specific control packets is exceeded.
	zyErrdisableRecovery	1.3.6.1.4.1.890.1.15.3.24.4.2	This trap is sent when the Switch ceases the action taken on a port, such as shutting down the port or discarding packets on the port, after the specified recovery interval.
dyinggasp	zyHwMonitorDyingGasp	1.3.6.1.4.1.890.1.15.3.26.2.5	The trap is sent when the device power goes below the normal value.
powersource	zyHwMonitorPowerSourceAbnormal	1.3.6.1.4.1.890.1.15.3.26.2.10	This trap is sent when the power source has an error.
	zyHwMonitorPowerSourceAbnormalRecovered	1.3.6.1.4.1.890.1.15.3.26.2.11	This trap is sent when the power source recovers to a normal status.
loginrecord	zyAccessControlLoginRecord	1.3.6.1.4.1.890.1.15.3.9.4.1	This trap is sent when users log in.
	zyAccessControlLogoutRecord	1.3.6.1.4.1.890.1.15.3.9.4.2	This trap is sent when users log out.
	zyAccessControlLoginFail	1.3.6.1.4.1.890.1.15.3.9.4.3	This trap is sent when users fail in login.

Table 231 SNMP Stacking Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
Channel	zyStackingChannelUp	1.3.6.1.4.1.890.1.15.3.97.4.1	stacking channel up
	zyStackingChannelDown	1.3.6.1.4.1.890.1.15.3.97.4.2	stacking channel down
Slot	zyStackingSlotAttach	1.3.6.1.4.1.890.1.15.3.97.4.3	stacking slot attached success
	zyStackingSlotDetach	1.3.6.1.4.1.890.1.15.3.97.4.4	stacking slot detached
Master	zyStackingNewMaster	1.3.6.1.4.1.890.1.15.3.97.4.5	backup takeover as master
Upgrade Firmware	zyStackingUpgradeFirmwareFail	1.3.6.1.4.1.890.1.15.3.97.4.6	Upgrade Firmware fail with correspond slot ID.
Backup	zyStackingNewBackup	1.3.6.1.4.1.890.1.15.3.97.4.7	New Backup with correspond slot ID.
	zyStackingBackupTakeover	1.3.6.1.4.1.890.1.15.3.97.4.8	Replaced master with correspond slot ID.
Master	zyStackingNewMasterFromTakeover	1.3.6.1.4.1.890.1.15.3.97.4.9	New master from taking over with correspond slot ID.
Fail	zyStackingSyncConfFail	1.3.6.1.4.1.890.1.15.3.97.4.10	Sync. configuration fail with correspond slot ID.
	zyStackingSysRestoreConfFail	1.3.6.1.4.1.890.1.15.3.97.4.11	Stacking backup takeover resotre configuration fail.
	zyStackingSlotInitFail	1.3.6.1.4.1.890.1.15.3.97.4.12	Stacking Slot init fail.

Table 231 SNMP Stacking Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
Change	zyStackingSlotChangeIndex	1.3.6.1.4.1.890.1.15.3.97.4.13	Stacking change slot index.
	zyStackingPriorityChange	1.3.6.1.4.1.890.1.15.3.97.4.14	Staking prority change.
	zyStackingTopologyChange	1.3.6.1.4.1.890.1.15.3.97.4.15	Staking topology change.

Table 232 SNMP InterfaceTraps

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.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
autonegotiation	zyPortAutonegotiationFailed	1.3.6.1.4.1.890.1.15.3.61.3.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.
transceiver-ddm	zyTransceiverDdmiTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.1	This trap is sent when the transceiver temperature is above or below the normal operating range.
	zyTransceiverDdmiTxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.2	This trap is sent when the transmitted optical power is above or below the normal operating range.
	zyTransceiverDdmiRxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.3	This trap is sent when the received optical power is above or below the normal operating range.
	zyTransceiverDdmiVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.4	This trap is sent when the transceiver supply voltage is above or below the normal operating range.
	zyTransceiverDdmiTxBiasOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.5	This trap is sent when the transmitter laser bias current is above or below the normal operating range.
storm-control	zyPortStormControlTrap	1.3.6.1.4.1.890.1.15.3.78.2.1	This trap is sent when storm control is detected on a specific port. A packet filter action has been applied on the interface.

Table 232 SNMP InterfaceTraps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
zuld	zyZuldUnidirectionalDetected	1.3.6.1.4.1.890.1.15.3.110.3.1	This trap is sent when a unidirectional link is detected.
	zyZuldBidirectionalRecovered	1.3.6.1.4.1.890.1.15.3.110.3.2	This trap is sent when the port which is shut down by ZULD becomes active again.

Table 233 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.
	zyAaaAuthenticationFailure	1.3.6.1.4.1.890.1.15.3.8.3.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	zyRadiusServerAuthenticationServerNotReachable	1.3.6.1.4.1.890.1.15.3.71.2.1	This trap is sent when there is no response message from the RADIUS authentication server.
	zyTacacsServerAuthenticationServerUnreachable	1.3.6.1.4.1.890.1.15.3.83.2.1	This trap is sent when there is no response message from the TACACS+ authentication server.
authorization	zyAaaAuthorizationFailure	1.3.6.1.4.1.890.1.15.3.8.3.2	This trap is sent when management connection authorization failed.
accounting	zyRadiusServerAccountingServerNotReachable	1.3.6.1.4.1.890.1.15.3.71.2.2	This trap is sent when there is no response message from the RADIUS accounting server.
	zyTacacsServerAccountingServerUnreachable	1.3.6.1.4.1.890.1.15.3.83.2.2	This trap is sent when there is no response message from the TACACS+ accounting server.

Table 234 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

Table 235 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.
	zyMrstpNewRoot	1.3.6.1.4.1.890.1.15.3.52.3.1	This trap is sent when the MRSTP root switch changes.
	zyMstpNewRoot	1.3.6.1.4.1.890.1.15.3.53.3.1	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.
	zyMrstpTopologyChange	1.3.6.1.4.1.890.1.15.3.52.3.2	This trap is sent when the MRSTP topology changes.
	zyMstpTopologyChange	1.3.6.1.4.1.890.1.15.3.53.3.2	This trap is sent when the MSTP root switch changes.
mactable	zyMacForwardingTableFull	1.3.6.1.4.1.890.1.15.3.48.2.1	This trap is sent when more than 99% 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.
cfm	dot1agCfmFaultAlarm	1.3.111.2.802.1.1.8.0.1	The trap is sent when the Switch detects a connectivity fault.
classifier	zyAclV2ClassifierLogNotification	1.3.6.1.4.1.890.1.15.3.105.4.1	This trap is sent when the Switch detects classifier log information.

48.3.4 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 350 Management > Access Control > SNMP

The following table describes the labels in this screen.

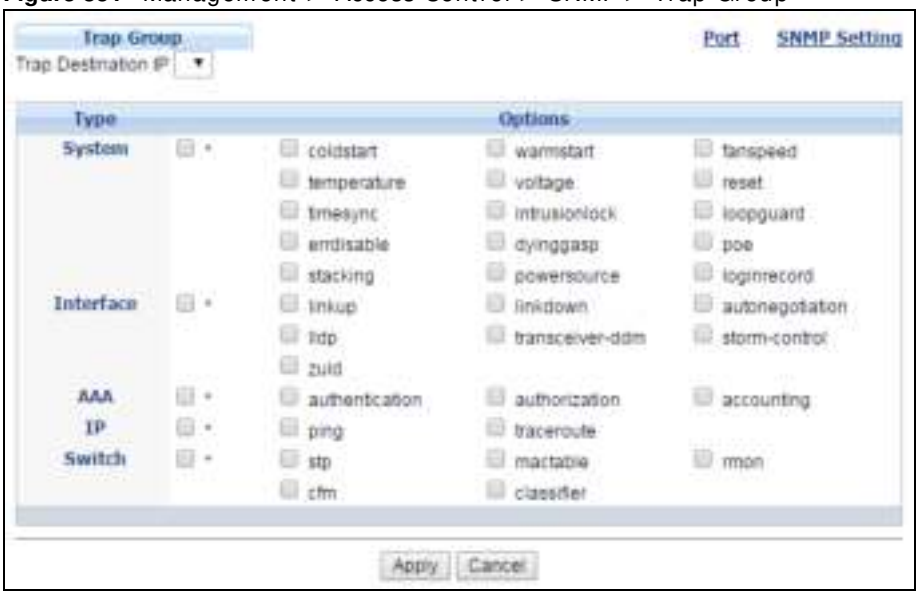
Table 236 Management > Access Control > SNMP

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 (**v2c**), SNMP version 3 (**v3**) or both (**v3v2c**). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNext- requests from the management station. The **Get Community** string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the **Set Community** string, which is the password for the incoming Set- requests from the management station. The **Set Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the **Trap Community** string, which is the password sent with each trap to the SNMP manager. The **Trap Community** 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 IP 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. Note: This username must match an existing account on the Switch (configured in the **Management > Access Control > SNMP > User** screen).
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

48.3.5 Configuring SNMP Trap Group

From the **SNMP** screen, click **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 351 Management > Access Control > SNMP > Trap Group



The following table describes the labels in this screen.

Table 237 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 **SNMP Setting** 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 Section 48.3.3 on page 461 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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

48.3.6 Enabling/Disabling Sending of SNMP Traps on a Port

From the **SNMP > Trap Group** screen, click **Port** to view the screen as shown. Use this screen to set whether a trap received on the port(s) would be sent to the SNMP manager.

Figure 352 Management > Access Control > SNMP > Trap Group > Port (Standalone mode)

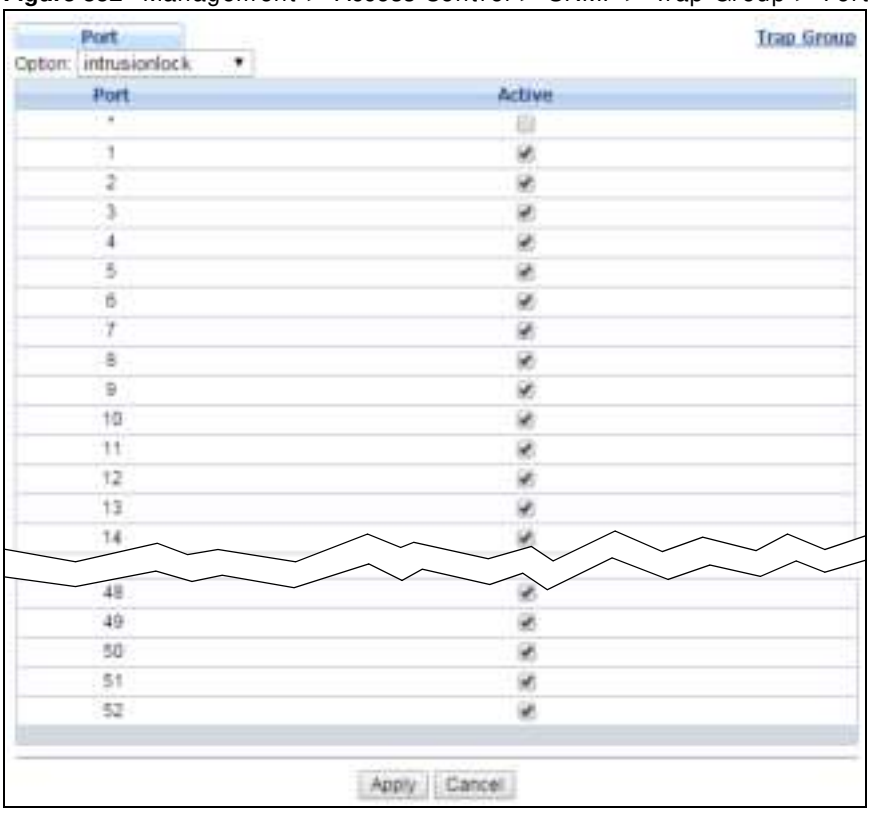
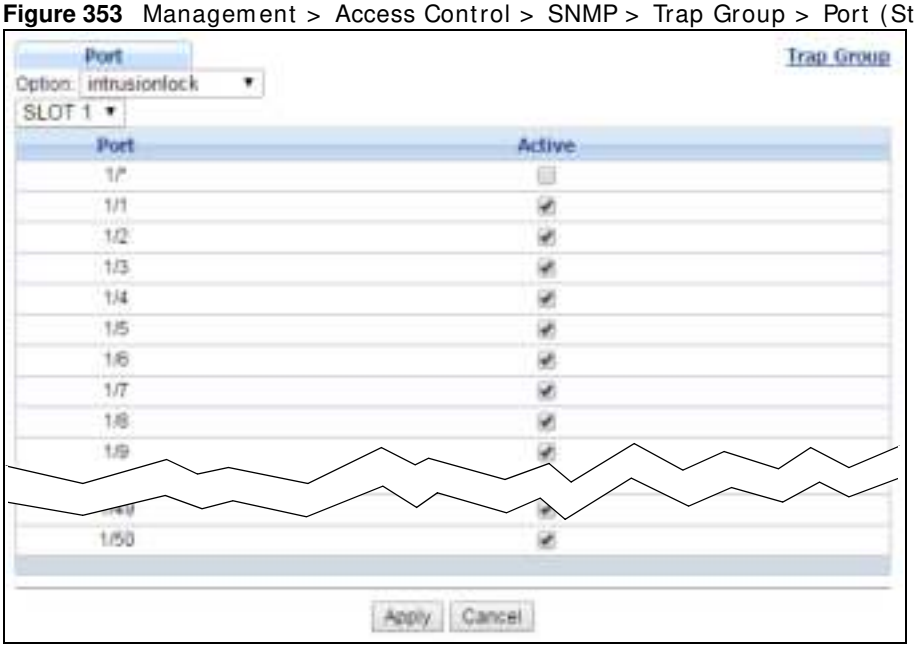


Figure 353 Management > Access Control > SNMP > Trap Group > Port (Stacking mode)



The following table describes the labels in this screen.

Table 238 Management > Access Control > SNMP > Trap Group > Port

LABEL	DESCRIPTION
Option	Select the trap type you want to configure here.
Slot	Select the slot number that represents the Switch in a stack.

Table 238 Management > Access Control > SNMP > Trap Group > Port (continued)

LABEL	DESCRIPTION
Port	This field displays a port number. In stacking mode, the first number represents the slot and the second the port number.
1/*	Settings in this row apply to all ports for the Switch represented by the slot ID (in stacking mode). Use this row only if you want to make some of the 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 the sending of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. Clear this check box to disable the sending of SNMP traps on this port.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

48.3.7 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 354 Management > Access Control > SNMP > User

The following table describes the labels in this screen.

Table 239 Management > Access Control > SNMP > User

LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.
Username	Specify the username of a login account on the Switch.

Table 239 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • **noauth** -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. • **auth** - to implement an authentication algorithm for SNMP messages sent by this user. • **priv** - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: 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. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • **DES** - 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. • **AES** - 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.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. **admin** - Members of this group can perform all types of system configuration, including the management of administrator accounts. **readwrite** - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. **readonly** - Members of this group have read rights only, meaning the user can collect information from the Switch.
Add	Click this to create a new entry or to update an existing one. This saves 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is a read-only number identifying a login account on the Switch. Click on an index number to view more details and edit an existing account.
Username	This field displays the username of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.

Table 239 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to begin configuring this screen afresh.

48.4 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.

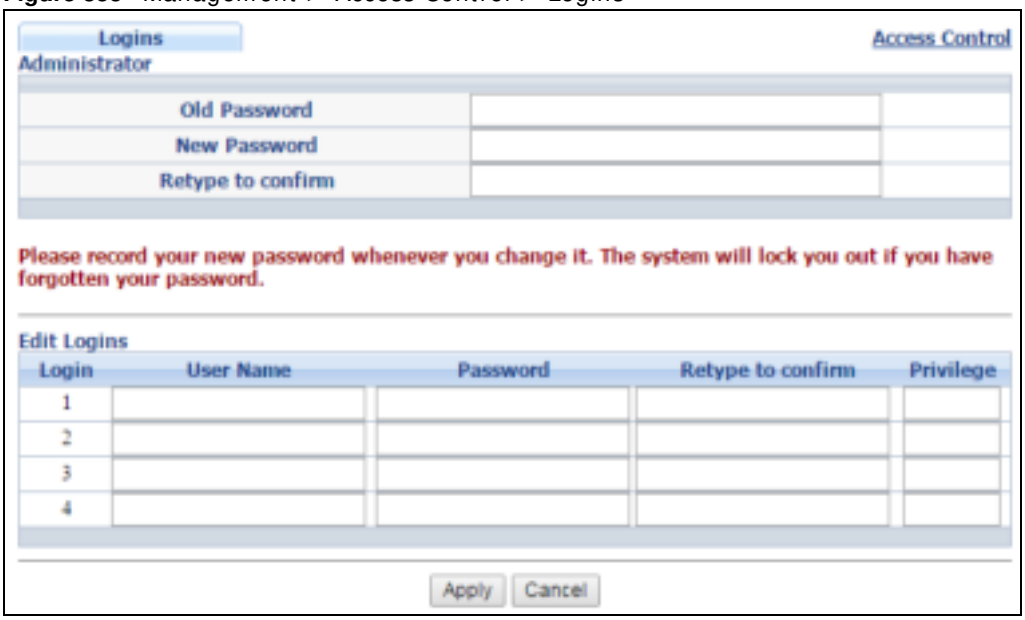
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

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.

Figure 355 Management > Access Control > Logins



The following table describes the labels in this screen.

Table 240 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 (**1234** is the default password when shipped).

Table 240 Management > Access Control > Logins (continued)

LABEL	DESCRIPTION
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 Ethernet Switch 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
Privilege	Type the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown below. • 0 - Display basic system information. • 3 - Display configuration or status. • 13 - Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. • 14 - Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he/she can run commands that requires privilege level of 5 or less but not more.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

48.5 SSH Overview

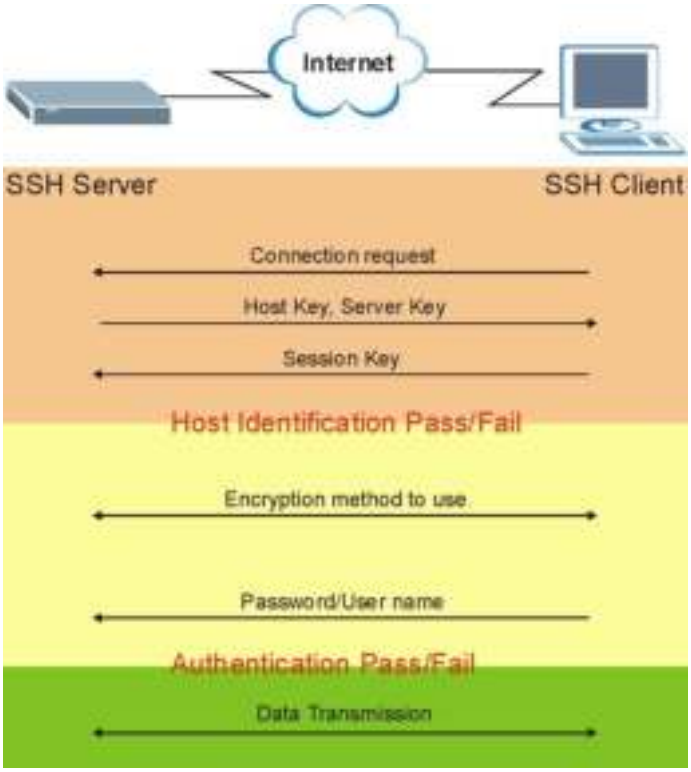
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 356 SSH Communication Example

48.6 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 357 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.

48.7 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.

48.7.1 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.

48.8 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.

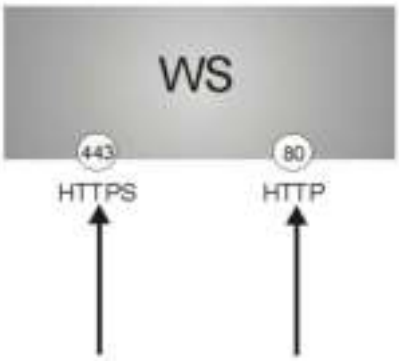
HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only 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 Certificate Authority (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 358 HTTPS Implementation



Note: If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

48.9 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.

48.9.1 Internet Explorer Warning Messages

48.9.1.1 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.

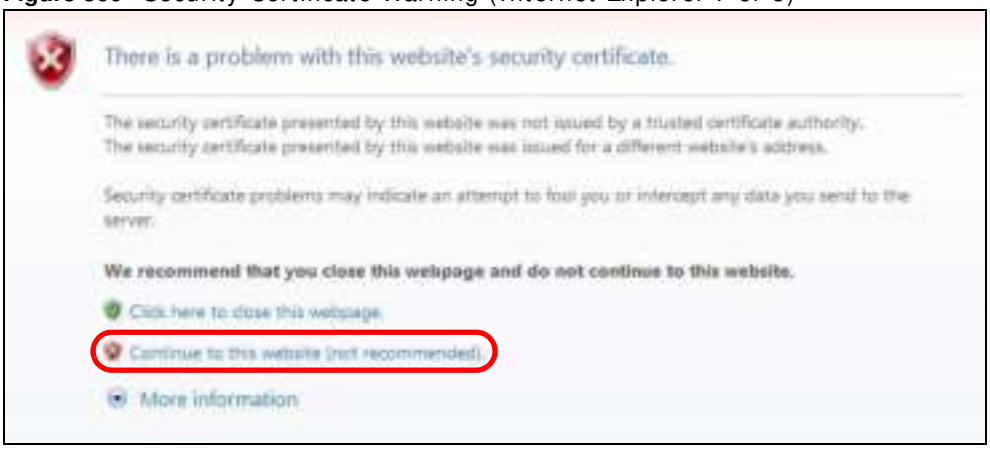
You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 359 Security Alert Dialog Box (Internet Explorer 6)

48.9.1.2 Internet Explorer 7 or 8

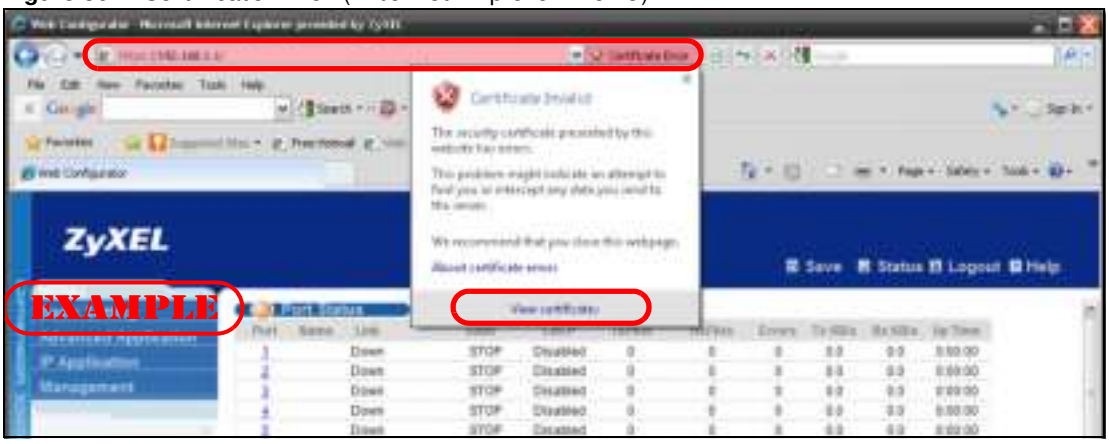
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the web configurator login screen.

Figure 360 Security Certificate Warning (Internet Explorer 7 or 8)



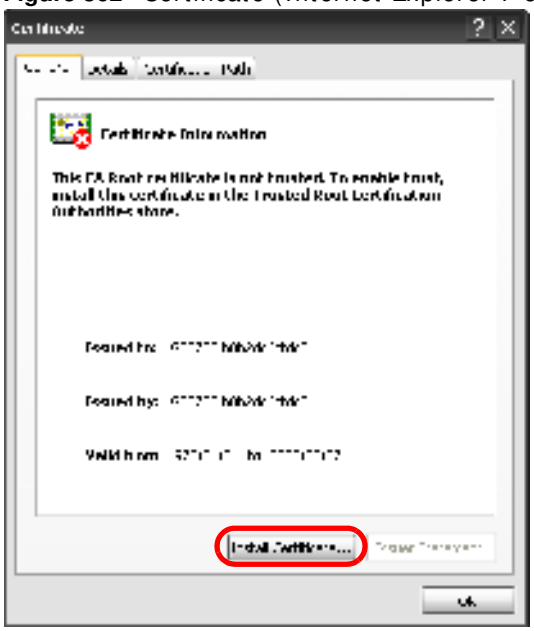
After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 361 Certificate Error (Internet Explorer 7 or 8)



Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

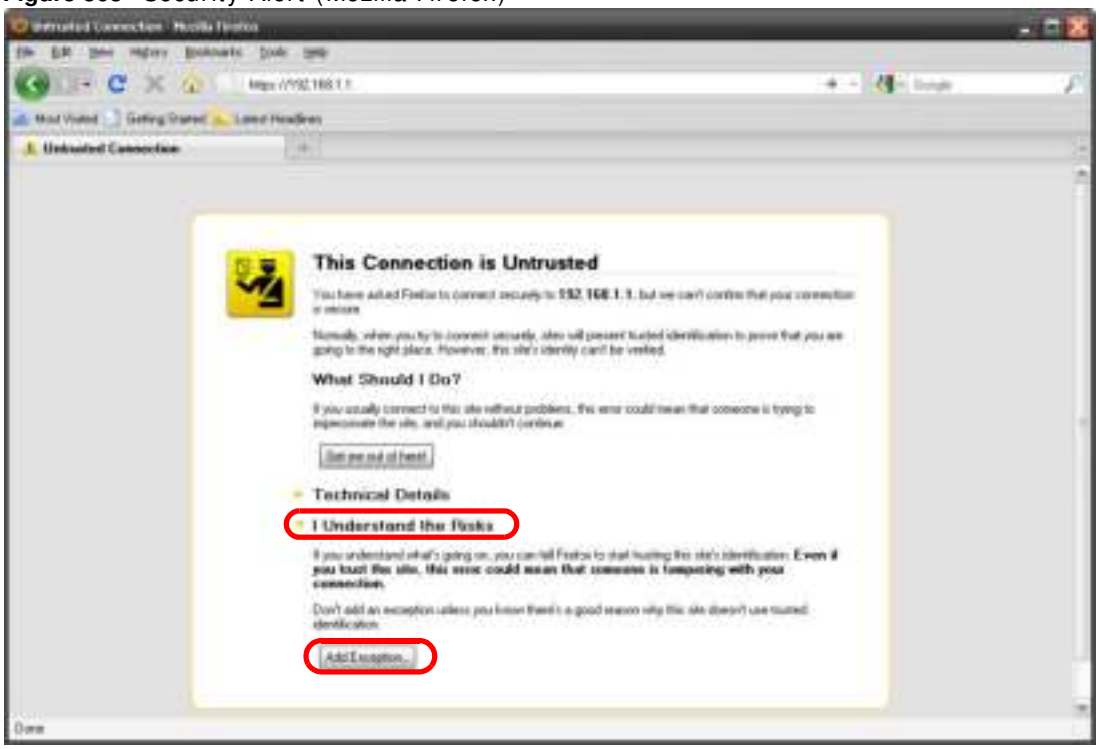
Figure 362 Certificate (Internet Explorer 7 or 8)



48.9.2 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 363 Security Alert (Mozilla Firefox)



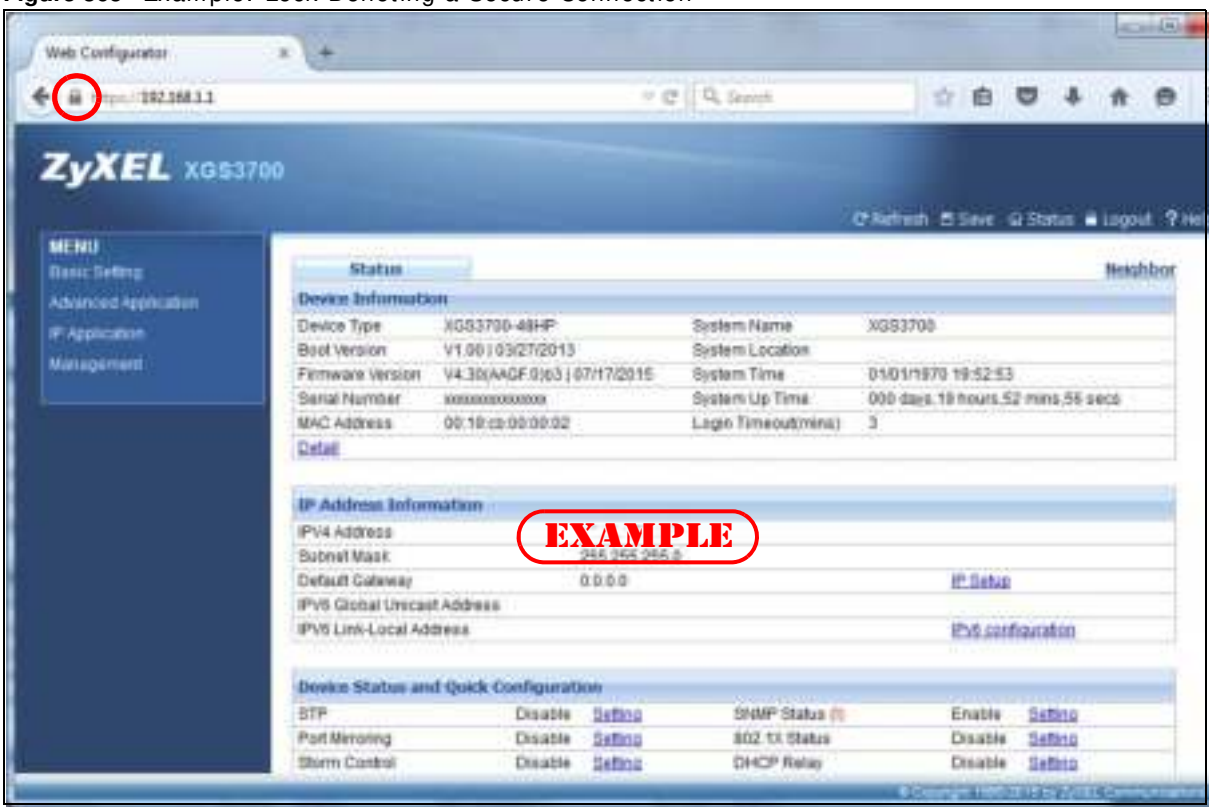
Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

Figure 364 Security Alert (Mozilla Firefox)

48.9.3 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 or next to the website address denotes a secure connection.

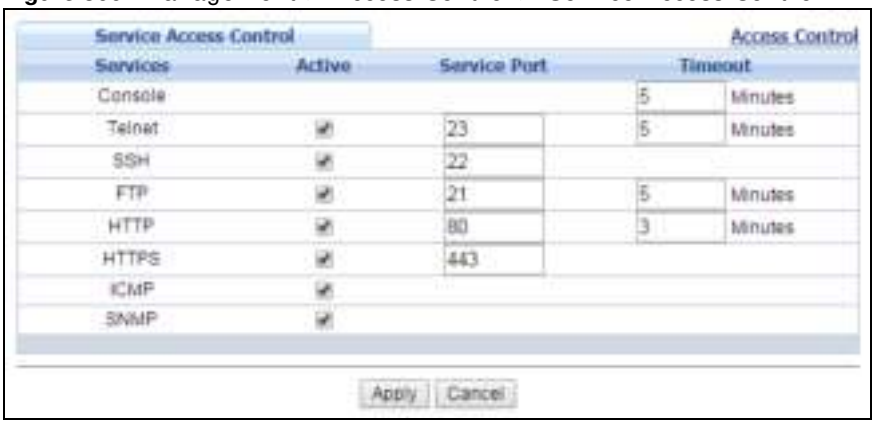
Figure 365 Example: Lock Denoting a Secure Connection



48.10 Service 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 **Access Control** to go back to the main **Access Control** screen.

Figure 366 Management > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 241 Management > Access Control > Service Access Control

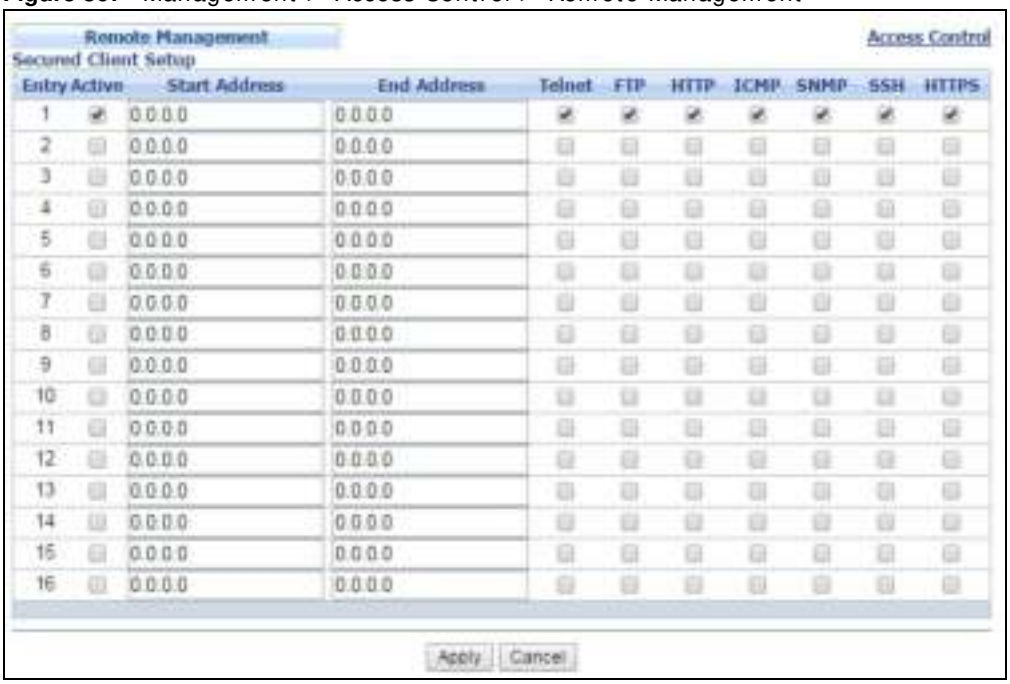
LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Service Port** 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 (from 1 to 255) a management session 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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

48.11 Remote Management

From the **Access Control** screen, display the **Remote Management** 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 367 Management > Access Control > Remote Management



The following table describes the labels in this screen.

Table 242 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 IP 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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

49

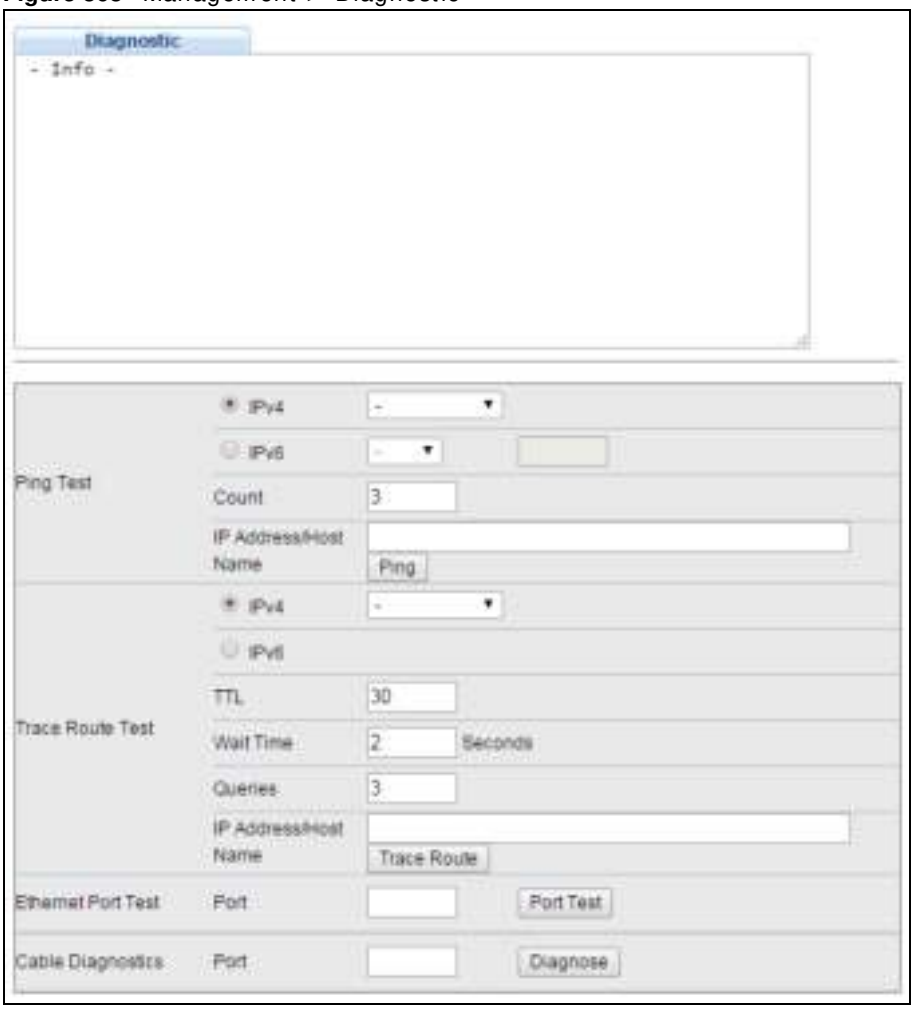
Diagnostic

This chapter explains the **Diagnostic** screen. You can use this screen to help you identify problems.

49.1 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 368 Management > Diagnostic



The following table describes the labels in this screen.

Table 243 Management > Diagnostic

LABEL	DESCRIPTION
Ping Test	
IPv4	Select this option if you want to ping an IPv4 address, and select which traffic flow (**in-band** or **out-of-band**) the Switch is to send ping frames. If you select **in-band**, the Switch sends the frames to all ports except the management port (labelled **MGMT**). If you select **out-of-band**, the Switch sends the frames to the management port (labelled **MGMT**). Otherwise, select **-** to send ping requests to all VLANs on the Switch.
IPv6	Select this option if you want to ping an IPv6 address. You can also select **vlan** and specify the ID number of the VLAN to which the Switch is to send ping requests. Otherwise, select **-** to send ping requests to all VLANs on the Switch.
Count	Enter the number of ICMP Echo Request (ping) messages the Switch continuously sends.
IP Address/ Host Name	Type the IP address or host name of a device that you want to ping in order to test a connection. Click **Ping** to have the Switch ping the IP address.
Trace Route Test	
IPv4	Select this option if you want to trace the route packets take to a device with an IPv4 address, and select **in-band** or **out-of-band** on which the Switch traces the path. Otherwise, select **-** to trace the path on any VLAN.
IPv6	Select this option if you want to trace the route packets take to a device with an IPv6 address.
TTL	Enter the Time To Live (TTL) value for the ICMP Echo Request packets. This is to set the maximum number of the hops (routers) a packet can travel through. Each router along the path will decrement the TTL value by one and forward the packets. When the TTL value becomes zero and the destination is not found, the router drops the packets and informs the sender.
Wait Time	Specify how many seconds the Switch waits for a response to a probe before running another traceroute.
Queries	Specify how many times the Switch performs the traceroute function.
IP Address/ Host Name	Enter the IP address or host name of a device to which you want to perform a traceroute. Click **Trace Route** to have the Switch perform the traceroute function. This determines the path a packet takes to the specified device.
Ethernet Port Test	Enter a port number and click **Port Test** to perform an internal loopback test.
Cable Diagnostics	Enter a port number and click **Diagnose** to perform a physical wire-pair test of the Ethernet connections on the specified port(s). The following fields display when you diagnose a port.
Port	This is the number of the physical Ethernet port on the Switch.
Channel	An Ethernet cable usually has four pairs of wires. A 10BASE-T or 100BASE-TX port only use and test two pairs, while a 1000BASE-T port requires all four pairs. This displays the descriptive name of the wire-pair in the cable.

Table 243 Management > Diagnostic (continued)

LABEL	DESCRIPTION
Pair status	**Ok**: The physical connection between the wire-pair is okay. **Open**: There is no physical connection (an open circuit detected) between the wire-pair. **Short**: There is an short circuit detected between the wire-pair. **Unknown**: The Switch failed to run cable diagnostics on the cable connected this port. **Unsupported**: The port is a fiber port or it is not active.
Cable length (m)	This displays the total length of the Ethernet cable that is connected to the port when the **Pair status** is **Ok** and the Switch chipset supports this feature. This shows **N/A** if the **Pair status** is **Open** or **Short**. Check the **Distance to fault**. This shows **Unsupported** if the Switch chipset does not support to show the cable length.
Distance to fault (m)	This displays the distance between the port and the location where the cable is open or shorted. This shows **N/A** if the **Pair status** is **Ok**. This shows **Unsupported** if the Switch chipset does not support to show the distance.

50

System Log

50.1 Overview

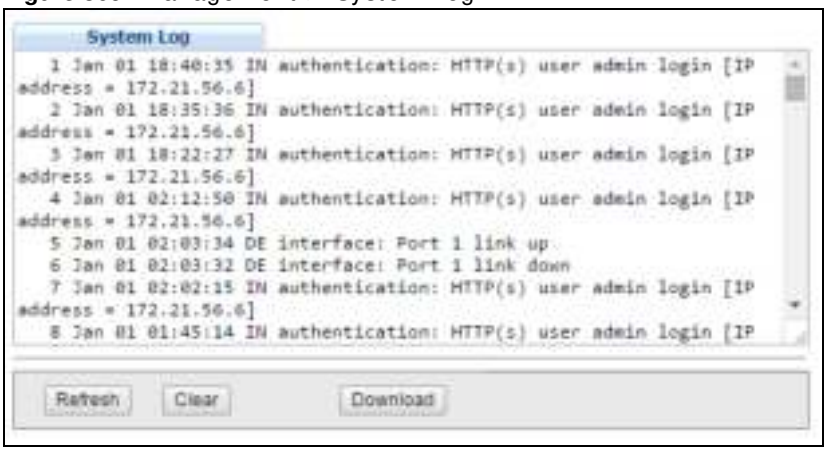
A log message stores the information for viewing.

50.2 System Log

Click **Management > System Log** in the navigation panel to open this screen. Use this screen to check current system logs.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

Figure 369 Management > System Log



The summary table shows the time the log message was recorded and the reason the log message was generated. Click **Refresh** to update this screen. Click **Clear** to clear the whole log, regardless of what is currently displayed on the screen. Click **Download** to save the log to your computer.

51

Syslog Setup

This chapter explains the syslog screens.

51.1 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 244 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.

51.2 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 and configure a list of external syslog servers.

Figure 370 Management > Syslog Setup

The following table describes the labels in this screen.

Table 245 Management > Syslog Setup

LABEL	DESCRIPTION
Syslog	Select **Active** 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 **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Syslog Server Setup	
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 IP 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.

Table 245 Management > Syslog Setup

LABEL	DESCRIPTION
Add	Click **Add** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** 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 **Yes** if the device is to send logs to the syslog server. **No** 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.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click **Delete** to remove the selected entry(ies).
Cancel	Click Cancel to begin configuring this screen afresh.

52

Cluster Management

This chapter introduces cluster management.

52.1 Clustering Management Status Overview

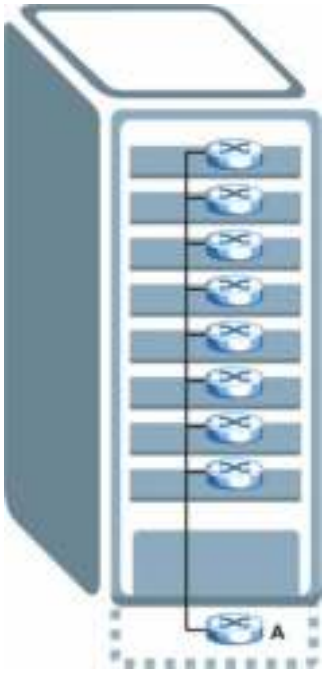
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 246 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Cluster member models must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The cluster manager is the Switch through which you manage the cluster member switches.
Cluster Members	Cluster members are the switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 371 Clustering Application Example

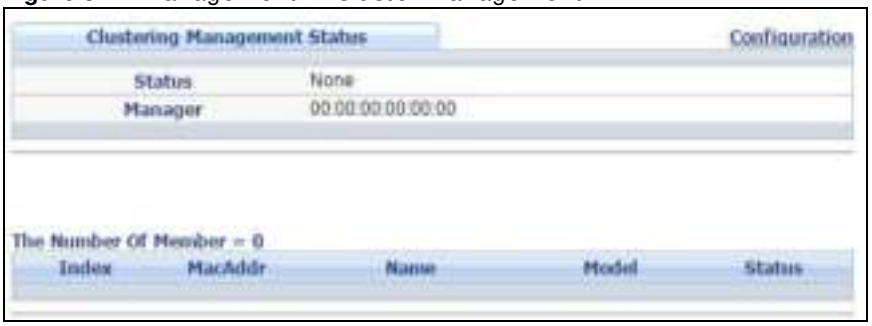


52.2 Cluster Management Status

Click **Management** > **Cluster Management** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 372 Management > Cluster Management



The following table describes the labels in this screen.

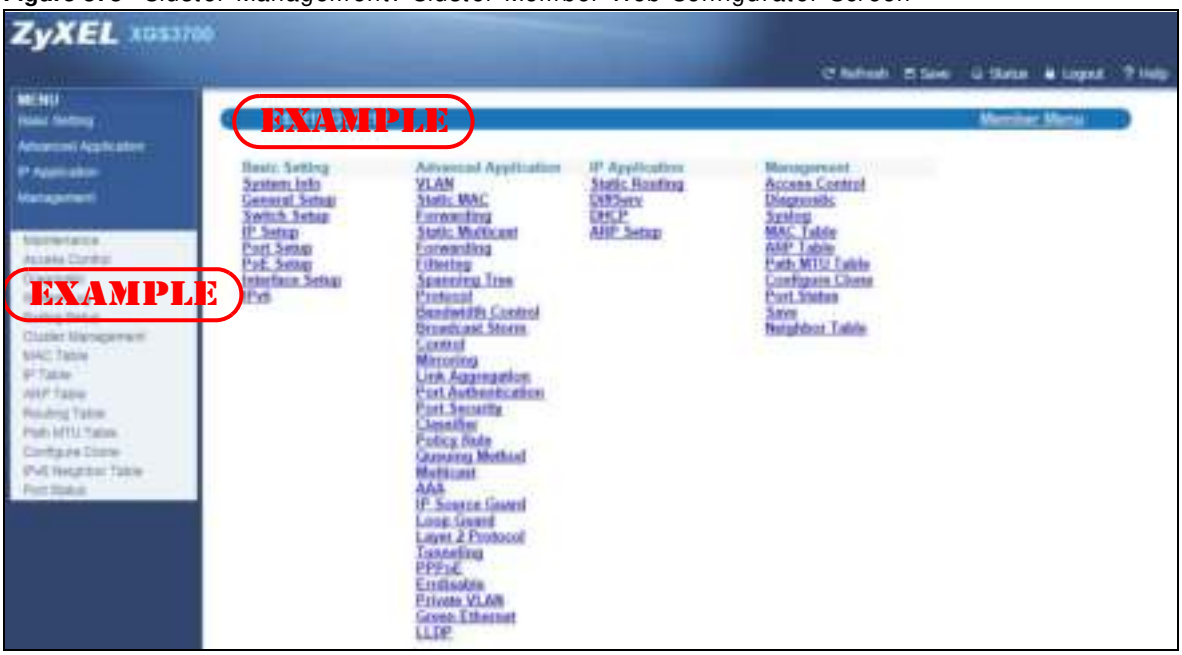
Table 247 Management > Cluster Management

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see Figure 373 on page 492).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This field displays the model name.
Status	This field displays: **Online** (the cluster member switch is accessible) **Error** (for example, the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

52.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 373 Cluster Management: Cluster Member Web Configurator Screen



52.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 374 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group       6173152 Jul 01 12:00 ras-0
--w--w--w-   1 owner    group       6173152 Jul 01 12:00 ras-1
-rw-rw-rw-   1 owner    group      33554432 Jul 01 12:00 config
--w--w--w-   1 owner    group             0 Jul 01 12:00 ras-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group             0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 410AAGB0.bin ras-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR ras-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

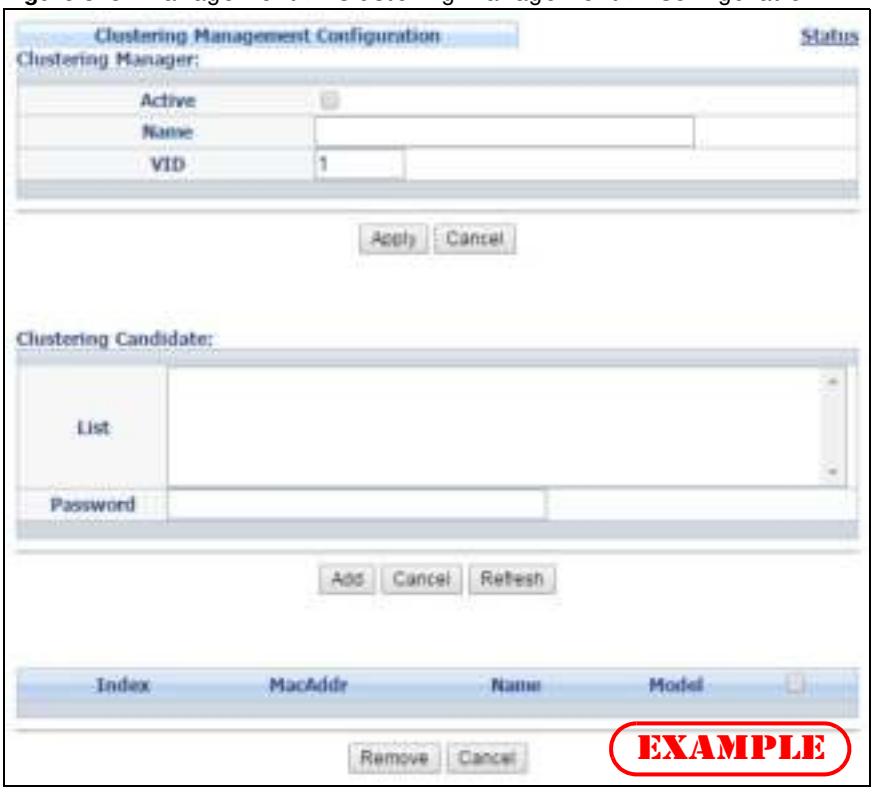
Table 248 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter “admin”.
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch’s firmware and configuration file.
410AAGB0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
ras-00-a0-c5-01-23-46	This is the cluster member switch’s firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch’s configuration file name as seen in the cluster manager switch.

52.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 375 Management > Clustering Management > Configuration



The following table describes the labels in this screen.

Table 249 Management > Clustering Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager**. You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Remove	Click the **Remove** button to remove the selected cluster member switch(es) from the cluster.
Cancel	Click **Cancel** to begin configuring this screen afresh.

53

MAC Table

This chapter introduces the **MAC Table** screen.

53.1 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. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's **MAC Table**. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

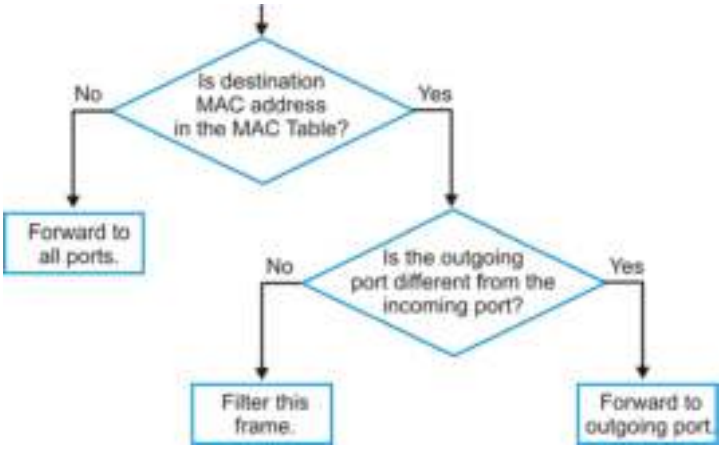
The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1 The Switch examines a received frame and learns the port from 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 then the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
- 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.

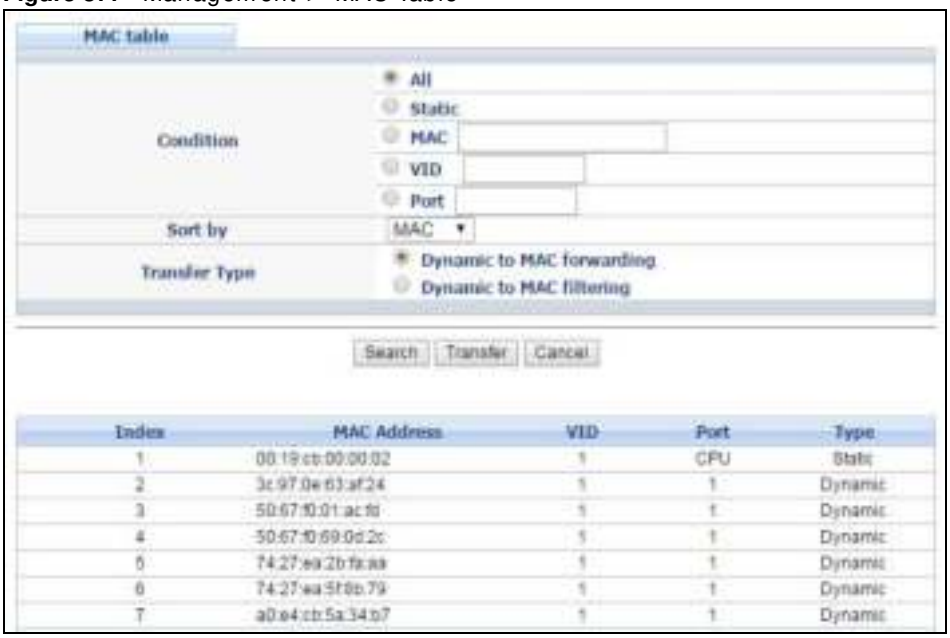
Figure 376 MAC Table Flowchart



53.2 Viewing the MAC Table

Click **Management** > **MAC Table** in the navigation panel to display the following screen. Use this screen to search specific MAC addresses. You can also directly add dynamic MAC address(es) into the static MAC forwarding table or MAC filtering table from the MAC table using this screen.

Figure 377 Management > MAC Table



The following table describes the labels in this screen.

Table 250 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select **All** to display all MAC addresses in the MAC table. Select **Static** to only display static MAC address(es) in this screen. Select **MAC** and enter a valid MAC address (six hexadecimal character pairs) to display the MAC address information in this screen. Select **VID** and type a VLAN identification number to display all MAC addresses in the VLAN. Select **Port** and type the number of a port to display all MAC addresses learned from the port.
Sort by	Select this to display and arrange the data according to MAC address (**MAC**), VLAN group (**VID**) or port number (**Port**). The information is then displayed in the summary table below.
Transfer Type	Select **Dynamic to MAC forwarding** and click **Transfer** to add the relative dynamic MAC address(es) you select the criteria here into the static MAC forwarding table (see Section 8.2 on page 124). The type of the MAC address(es) will be changed to “static”. Select **Dynamic to MAC filtering** and click **Transfer** to add the relative dynamic MAC address(es) you make the search here into the static MAC filtering table (see Section 10.1 on page 130). The MAC address(es) will be removed from the MAC table and all traffic sent from the MAC address(es) will be blocked by the Switch.
Search	Click this to search data in the MAC table according to your input criteria.
Transfer	Click this to perform the MAC address transferring you selected in the **Transfer Type** field.

Table 250 Management > MAC Table (continued)

LABEL	DESCRIPTION
Cancel	Click this to begin configuring the search criteria afresh.
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. In stacking mode, the first number represents the slot and the second the port number.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

54

IP Table

This chapter introduces the IP table.

54.1 IP Table Overview

The **IP Table** screen shows how packets are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the IP address of the device is shown on the Switch's **IP Table**. The **IP Table** also shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

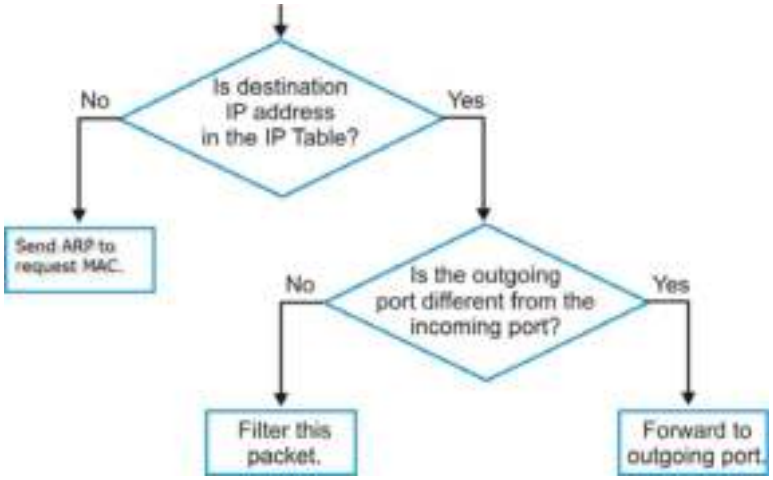
The Switch uses the **IP Table** to determine how to forward packets. See the following figure.

1 The Switch examines a received packet and learns the port from which this source IP address came.

2 The Switch checks to see if the packet's destination IP address matches a source IP address already learned in the **IP Table**.

- If the Switch has already learned the port for this IP address, then it forwards the packet to that port.
- If the Switch has not already learned the port for this IP address, then the packet is flooded to all ports. Too much port flooding leads to network congestionthen the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
- If the Switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

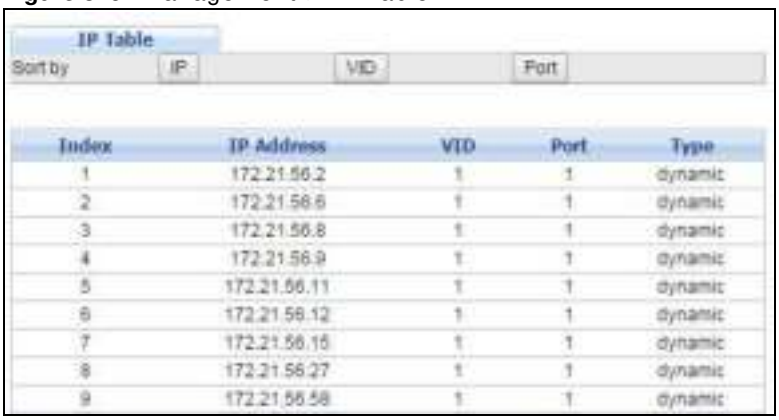
Figure 378 IP Table Flowchart



54.2 Viewing the IP Table

Click **Management** > **IP Table** in the navigation panel to display the following screen.

Figure 379 Management > IP Table



The following table describes the labels in this screen.

Table 251 Management > IP Table

LABEL	DESCRIPTION
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.
IP	Click this button to display and arrange the data according to IP 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.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays **CPU** to indicate the IP address belongs to the Switch. In stacking mode, the first number represents the slot and the second the port number.
Type	This shows whether the IP address is **dynamic** (learned by the Switch) or **static** (belonging to the Switch).

55

ARP Table

This chapter introduces ARP Table.

55.1 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.

55.1.1 How ARP Works

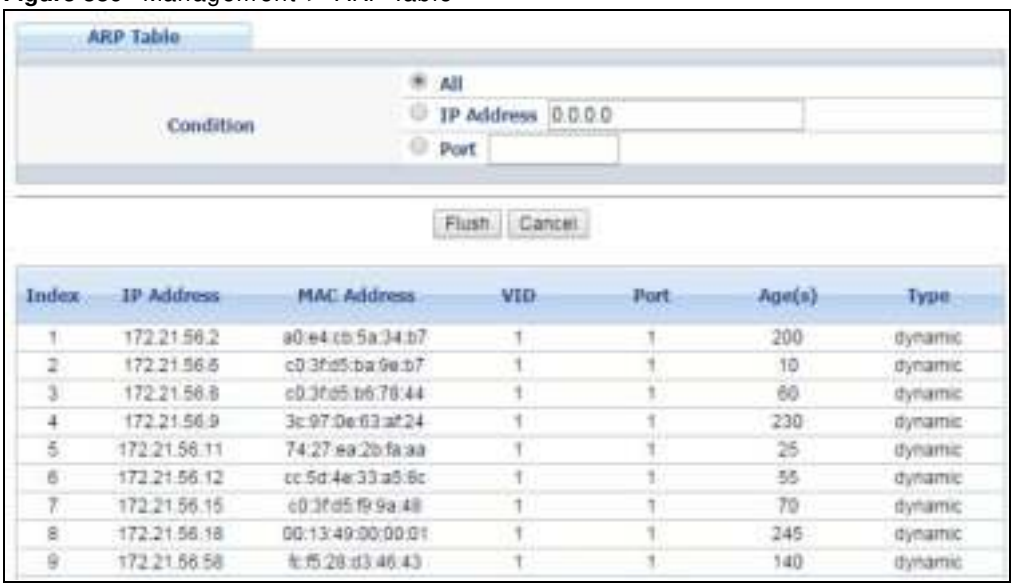
When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and if it finds the address, it sends it to the device.

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.

55.2 The ARP Table Screen

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) and remove specific dynamic ARP entries.

Figure 380 Management > ARP Table



The following table describes the labels in this screen.

Table 252 Management > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the Switch to remove ARP entries when you click **Flush**. Select **All** to remove all of the dynamic entries from the ARP table. Select **IP Address** and enter an IP address to remove the dynamic entries learned with the specified IP address. Select **Port** and enter a port number to remove the dynamic entries learned on the specified port.
Flush	Click **Flush** to remove the ARP entries according to the condition you specified.
Cancel	Click **Cancel** to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. **CPU** means this IP address is the Switch's management IP address. In stacking mode, the first number represents the slot and the second the port number.
Age(s)	This field displays how long (in seconds) an entry can still remain in the ARP table before it ages out and needs to be relearned. This shows **0** for a static entry.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (manually configured in the **Basic Setting > IP Setup** or **IP Application > ARP Setup > Static ARP** screen).

56

Routing Table

This chapter introduces the routing table.

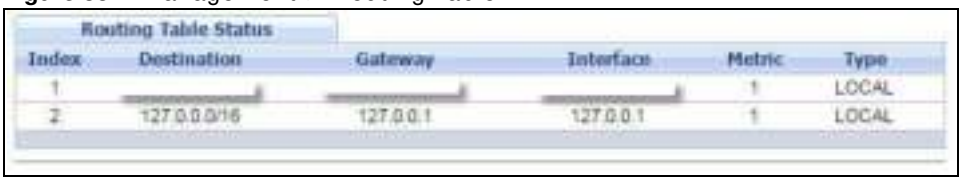
56.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach.

56.2 Viewing the Routing Table Status

Use this screen to view routing table information. Click **Management** > **Routing Table** in the navigation panel to display the screen as shown.

Figure 381 Management > Routing Table



The following table describes the labels in this screen.

Table 253 Management > Routing Table

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route. **STATIC** - added as a static entry.

57

Path MTU Table

This chapter introduces the IPv6 Path MTU table.

57.1 Path MTU Overview

The largest size (in bytes) of a packet that can be transferred over a data link is called the maximum transmission unit (MTU). The Switch uses Path MTU Discovery to discover Path MTU (PMTU), that is, the minimum link MTU of all the links in a path to the destination. If the Switch receives an ICMPv6 Packet Too Big error message after sending a packet, it fragments the next packet according to the suggested MTU in the error message.

57.2 Viewing the Path MTU Table

Use this screen to view IPv6 path MTU information on the Switch. Click **Management** > **Path MTU Table** in the navigation panel to display the screen as shown.

Figure 382 Management > Path MTU Table

The following table describes the labels in this screen.

Table 254 Management > Path MTU Table

LABEL	DESCRIPTION
Path MTU aging time	This field displays how long an entry remains in the Path MTU table before it ages out and needs to be relearned.
Index	This field displays the index number of each entry in the table.
Destination Address	This field displays the destination IPv6 address of each path/entry.
MTU	This field displays the maximum transmission unit of the links in the path.
Expire	This field displays how long (in minutes) an entry can still remain in the Path MTU table before it ages out and needs to be relearned.

58

Configure Clone

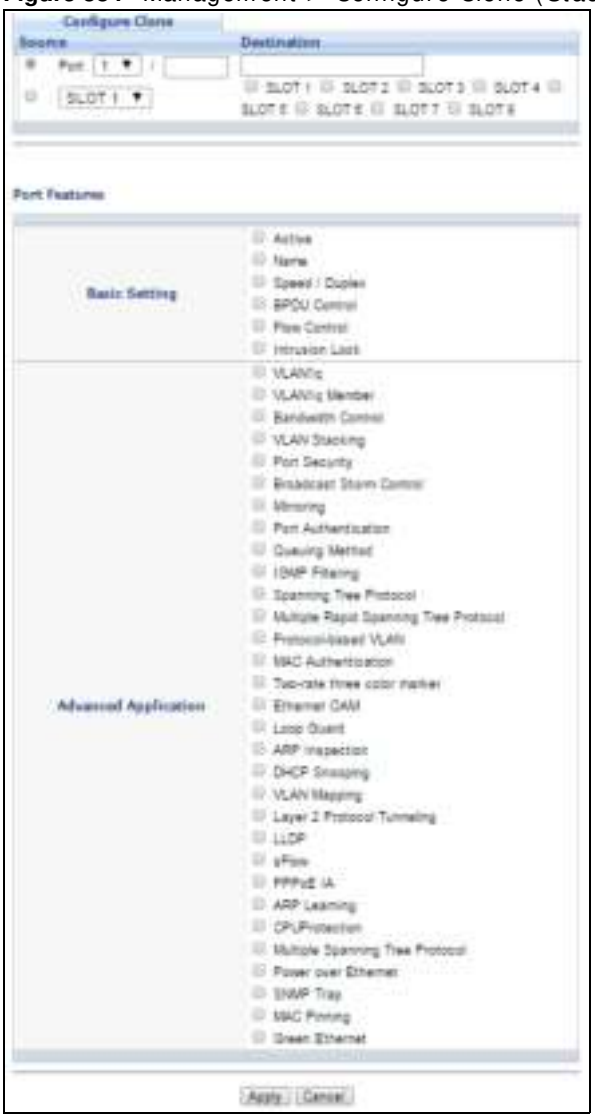
This chapter shows you how you can copy the settings of one port onto other ports.

58.1 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management** > **Configure Clone** to open the following screen.

Figure 383 Management > Configure Clone (Standalone)

Figure 384 Management > Configure Clone (Stacking)



The following table describes the labels in this screen.

Table 255 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination	In stacking mode, a port is defined by a slot ID representing the Switch in the stack and a port number.
Port / Slot (Stacking)	Select the source port and slot (in stacking mode) under the **Source** label. This port's attributes are copied. Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a hyphen. For example, **2, 4, 6** indicates that ports 2, 4 and 6 are the destination ports. **2-6** indicates that ports 2 through 6 are the destination ports. In stacking mode, you can select multiple destination slots.
Basic Setting	Select which port settings (configured in the **Basic Setting** menus) should be copied to the destination port(s).

Table 255 Management > Configure Clone (continued)

LABEL	DESCRIPTION
Advanced Application	Select which port settings (configured in the **Advanced Application** menus) should be copied to the destination ports.
Apply	Click **Apply** 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 **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

59

IPv6 Neighbor Table

This chapter introduces the IPv6 neighbor table.

59.1 IPv6 Neighbor Table Overview

An IPv6 host is required to have a neighbor table. If there is an address to be resolved or verified, the Switch 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 table. You can also manually create a static IPv6 neighbor entry using the **Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup** screen.

When the Switch needs to send a packet, it first consults other table to determine the next hop. Once the next hop IPv6 address is known, the Switch looks into the neighbor table 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 table 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.

59.2 Viewing the IPv6 Neighbor Table

Use this screen to view IPv6 neighbor information on the Switch. Click **Management** > **IPv6 Neighbor Table** in the navigation panel to display the screen as shown.

Figure 385 Management > IPv6 Neighbor Table

The following table describes the labels in this screen.

Table 256 Management > IPv6 Neighbor Table

LABEL	DESCRIPTION
Index	This field displays the index number of each entry in the table.
Interface	This field displays the ID number of the IPv6 interface on which the IPv6 address is created or through which the neighboring device can be reached.
Neighbor Address	This field displays the IPv6 address of the Switch or a neighboring device.
MAC	This field displays the MAC address of the IPv6 interface on which the IPv6 address is configure or the MAC address of the neighboring device.

Table 256 Management > IPv6 Neighbor Table (continued)

LABEL	DESCRIPTION
Status	This field displays whether the neighbor IPv6 interface is reachable. In IPv6, "reachable" means an IPv6 packet can be correctly forwarded to a neighbor node (host or router) and the neighbor can successfully receive and handle the packet. The available options in this field are: • reachable (R): The interface of the neighboring device is reachable. (The Switch has received a response to the initial request.) • stale (S): The last reachable time has expired and the Switch is waiting for a response to another initial request. The field displays this also when the Switch receives an unrequested response from the neighbor's interface. • delay (D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The Switch delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • probe (P): The Switch is sending request packets and waiting for the neighbor's response. • invalid (IV): The neighbor address is with an invalid IPv6 address. • unknown (?): The status of the neighboring interface can not be determined for some reason. • incomplete (I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. The interface of the neighboring device did not give a complete response.
Type	This field displays the type of an address mapping to a neighbor interface. The available options in this field are: • other (O): none of the following type. • local (L): A Switch interface is using the address. • dynamic (D): The IP address to MAC address can be successfully resolved using IPv6 Neighbor Discovery protocol. Is it similar as IPv4 ARP (Address Resolution protocol). • static (S): The interface address is statically configured.

60

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

60.1 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 3.3 on page 35.

2 Check the hardware connections. See Section 3.1 on page 30.

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.

60.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default in-band 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 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 44.

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 44.

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 IP address is 192.168.1.1.

- 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 3.3 on page 35.

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 44.

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 44.

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 48.11 on page 480). Computers not belonging to the secured client set cannot get permission to access the Switch.

60.3 Switch Configuration

I lost my configuration settings after I restart 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 47.6 on page 452 for more information about how to save your configuration.

A

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 257 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 www.zyxel.com) 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 257 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).

Table 257 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

B

IPv6

Overview

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 x 10^{38} IP addresses.

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`.

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.

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 258 Link-local Unicast Address Format

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

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.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 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.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 259 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 260 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0

Table 260 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

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.

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.

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 fffe 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.

Table 261

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

Table 262

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

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 Switch is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [1]another address which

combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

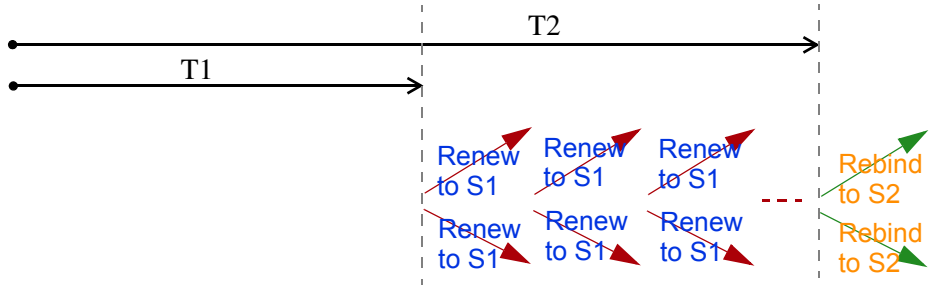
DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string,

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

such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Switch uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Switch passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device 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.

IPv6 Cache

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 onlink, 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.

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 listeners 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.

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. The router or switch then 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.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

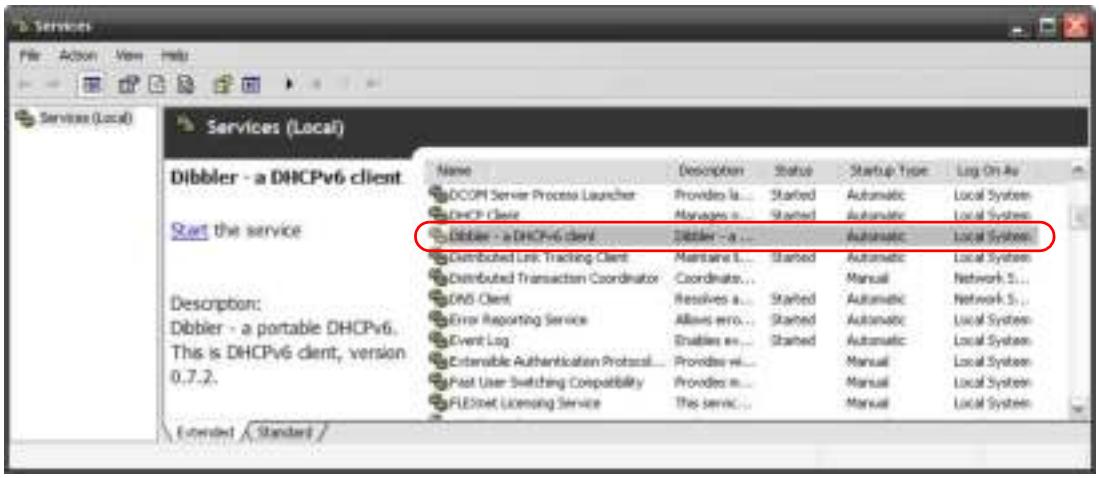
IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

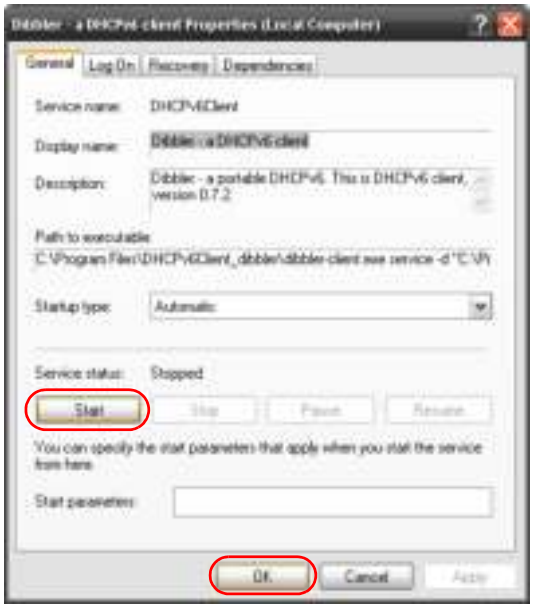
Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1. Install Dibbler and select the DHCPv6 client option on your computer.
2. After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.
4. Double click **Dibbler - a DHCPv6 client**.



5 Click **Start** and then **OK**.



6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

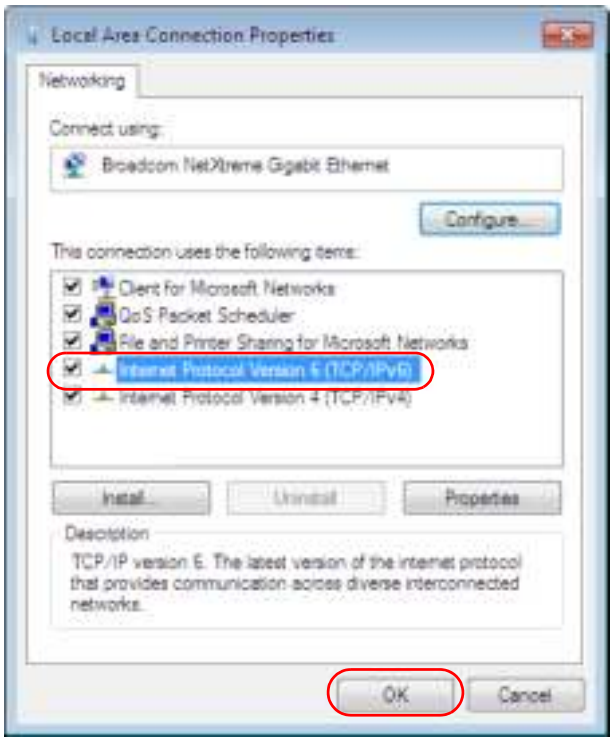
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

C

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See *http://www.zyxel.com/homepage.shtml* and also

http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Asia

China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- ZyXEL Kazakhstan

- http://www.zyxel.kz

Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- ZyXEL Philippines
- http://www.zyxel.com.ph

Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com/tw/zh/

Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Belarus

- ZyXEL BY
- http://www.zyxel.by

Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Czech Republic

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Finland

- ZyXEL Communications
- http://www.zyxel.fi

France

- ZyXEL France
- http://www.zyxel.fr

Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

Italy

- ZyXEL Communications Italy
- http://www.zyxel.it/

Latvia

- ZyXEL Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

Norway

- ZyXEL Communications
- http://www.zyxel.no

Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Russia

- ZyXEL Russia
- http://www.zyxel.ru

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- ZyXEL Communications ES Ltd
- http://www.zyxel.es

Sweden

- ZyXEL Communications

- http://www.zyxel.se

Switzerland

- Studerus AG
- http://www.zyxel.ch/

Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

- ZyXEL Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- ZyXEL Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- ZyXEL Communication Corporation

- http://www.zyxel.com/me/en/

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- http://www.zyxel.com/us/en/

Oceania

Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

D

Legal Information

Copyright

Copyright © 2015 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.

Regulatory Notice and Statement

United States of America

The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area

Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

European Union

The following information applies if you use the product within the European Union.

CE EMC statement

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

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

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.
- 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).
- DO NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- DO NOT use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not obstruct the device ventillation slots as insufficient airflow may harm your device.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  - Install the power supply before connecting the power cable to the power supply.

  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.
- The following warning statements apply, where the disconnect device is not incorporated in the equipment or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device shall be incorporated external to the equipment;

  - For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and shall be easily accessible.

Environment Statment

European Union - Disposal and Recycling Information

WEEE Directive

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

Environmental Product Declaration

台灣

以下訊息僅適用於產品銷售至台灣地區

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

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

安全警告

為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸

  任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。

  灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則

  - 先連接電源線至設備連，再連接電源。

  - 先斷開電源再拔除連接至設備的電源線。

  - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：

  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；

  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. 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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (ZyXEL Network Operating System) and ZON (ZyXEL One Network)are registered trademarks of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

Numbers

802.1P priority 72
802.3az 340

A

access control
  limitations 458
  login account 471
  remote management 480
  service port 479
  SNMP 459
accounting
  setup 257
address learning, MAC 112, 114
Address Resolution Protocol (ARP) 441, 500, 504, 506
administrator password 471
age 150
aggregator ID 177, 180
aging time 64
anti-arpscan 372
  blocked hosts 374
  host threshold 375
  status 373
  trusted hosts 374
applications
  bridging 22
  IEEE 802.1Q VLAN 23
  switched workgroup 22
ARP
  how it works 441, 500
  table 500
ARP (Address Resolution Protocol) 441, 500
ARP inspection 265, 297
  and MAC filter 297
  configuring 298
  syslog messages 298
  trusted ports 298
ARP scan 372
authentication
  and RADIUS 254
  setup 257
authorization
  privilege levels 260
  setup 257
automatic VLAN registration 102

B

back up, configuration file 451
basic settings 56
binding 265
binding table 265
  building 265
BPDU 378
BPDU (Bridge Protocol Data Units) 378
BPDU guard 378
  and Errdisable Recovery 378
  port status 378
BPDUs (Bridge Protocol Data Units) 133
Bridge Protocol Data Units 378
Bridge Protocol Data Units (BPDUs) 133

C

CDP 310
certifications
  viewing 537
CFI (Canonical Format Indicator) 101
changing the password 42
Cisco Discovery Protocol, see CDP
CIST 136
CIST (Common and Internal Spanning Tree) 134
Class of Service (CoS) 404
classifier 201, 205

and QoS 201
editing 206, 207
example 208
overview 201
setup 201, 205, 206, 207
viewing 206, 207
cloning a port See port cloning
cluster management 489
and switch passwords 494
cluster manager 489, 494
cluster member 489, 494
cluster member firmware upgrade 492
network example 489
setup 493
specification 489
status 490
switch models 489
VID 494
web configurator 491
cluster manager 489
cluster member 489
command interface 25
Common and Internal Spanning Tree (CIST) 134
Common and Internal Spanning Tree, See CIST 136
configuration 398
change running config 452
configuration file 44
backup 451
restore 44, 450
saving 452
configuration, saving 43
console port
settings 33
contact information 526
copying port settings, See port cloning
copyright 533
CPU management port 117
CPU protection
configuration 328
overview 325
current date 62
current time 62
customer support 526

D

daylight saving time 62
default gateway 421
default IP address 33
DHCP 413
client IP pool 421
configuration options 413
modes 413
relay agent 413
relay example 423
server 413
setup 420
DHCP (Dynamic Host Configuration Protocol) 413
DHCP relay option 82 296
DHCP snooping 265, 295
configuring 297
DHCP relay option 82 296
trusted ports 295
untrusted ports 295
DHCP snooping database 296
DHCP Unique IDentifier 427
DHCPv6
DHCP Unique IDentifier 427
diagnostics 482
Ethernet port test 483
ping 483
Differentiated Service (DiffServ) 404
DiffServ 404
activate 406
and TRTCM 410
DS field 404
DSCP 404
DSCP-to-IEEE802.1p mapping 411
network example 404
PHB 404
disclaimer 533
documentation
related 2
double-tagged frames 219
DS (Differentiated Services) 404
DSCP
DSCP-to-IEEE802.1p mapping 411
service level 404
what it does 404
DSCP (DiffServ Code Point) 404

DUID 427
dynamic link aggregation 175

E

EEE 340
egress port 120
Energy Efficient Ethernet 340
error disable detect 326, 330
error disable recovery
  configuration 331
  overview 325
Ethernet broadcast address 441, 500
Ethernet OAM 381
Ethernet port test 483
Ethernet ports
  default settings 31
external authentication server 254

F

Fan Module 34
fan speed 59, 60
FCC interference statement 533
file transfer using FTP
  command example 455
filename convention, configuration
  configuration
    file names 455
filtering 130
  rules 130
filtering database, MAC table 495
firmware 58
  upgrade 448, 492
flow control 72
  back pressure 72
  IEEE802.3x 72
forwarding
  delay 150
frames
  tagged 111
  untagged 111
front panel 30
FTP 25, 455
  file transfer procedure 456
  restrictions over WAN 457

G

GARP 102
GARP (Generic Attribute Registration Protocol) 102
GARP terminology 102
GARP timer 64, 102
general setup 61
getting help 45
GMT (Greenwich Mean Time) 62
Green Ethernet 340
GVRP 102, 111
  and port assignment 111
GVRP (GARP VLAN Registration Protocol) 102

H

hardware installation 26
hardware monitor 58, 59, 60
hardware overview 30
hello time 149
hops 150
HTTPS 474
  certificates 474
  implementation 474
  public keys, private keys 474
HTTPS example 475

I

IEEE 802.1p, priority 65
IEEE 802.1x
  activate 187, 192, 256
  reauthentication 189
IEEE 802.1x, port authentication 185
IGMP
  version 227
IGMP (Internet Group Management Protocol) 227

IGMP filtering 227
profile 235
profiles 231, 237, 238, 241, 242
IGMP leave timeout
fast 233
mormal 233
IGMP snooping 228
MVR 244
IGMP throttling 233
ingress port 120
Installation
Rack-mounting 27
installation
freestanding 26
precautions 27
Installing the Fan Module 34
Internet Protocol version 6, see IPv6
introduction 21
IP
interface 65, 66, 67, 431
routing domain 65
setup 65
IP address 66, 67
IP source guard 265
ARP inspection 265, 297
DHCP snooping 265, 295
static bindings 265
IP subnet mask 66, 67
IP table 498
how it works 498
IPv4 static route
configuration 397
IPv6 24, 517
addressing 517
EUI-64 519
global address 518
interface ID 519
link-local address 517
Neighbor Discovery Protocol 24, 517
ping 24, 517
prefix 427, 517
prefix length 427, 517
stateless autoconfiguration 519
unspecified address 518
IPv6 static route
configuration 398

L

L2PT 307
access port 308
CDP 307
configuration 308
encapsulation 307
LACP 307
MAC address 307
mode 308
overview 307
PAgP 307
point to point 307
STP 307
tunnel port 308
UDLD 307
VTP 307
LACP 175, 310
system priority 182
timeout 183
Layer 2 protocol tunneling, see L2PT
LEDs 35
limit MAC address learning 197
Link Aggregate Control Protocol (LACP) 175
link aggregation 175
dynamic 175
ID information 176
setup 177, 180
status 177
traffic distribution algorithm 177
traffic distribution type 180
Link Layer Discovery Protocol (LLDP) 343, 344
LLDP (Link Layer Discovery Protocol) 343
LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) 344
local port mirroring 162
lockout 43
login 37
password 42
login account
Administrator 471
non-administrator 471
login accounts 471
configuring via web configurator 471
multiple 471
number of 471
login password 472

loop guard 299
how it works 300
port shut down 300
probe packet 300
loop guard, vs STP 299

M

MAC (Media Access Control) 58
MAC address 58, 441, 500
maximum number per port 197, 198
MAC address learning 64, 112, 114, 124, 197
specify limit 197
MAC authentication 186
aging time 193
MAC filter
and ARP inspection 297
MAC freeze 197
MAC table 495
how it works 495
viewing 496
MAC-based VLAN 122
maintanence
configuration backup 451
firmware 448
restoring configuration 450
maintenance 447
current configuration 447
main screen 447
Management Information Base (MIB) 460
management port 33, 120
default IP address 33
managing the device
good habits 25
using FTP. See FTP.
using SNMP. See SNMP.
using Telnet. See command interface.
using the command interface. See command interface.
using the web configurator. See web configurator.
man-in-the-middle attacks 297
max
age 150
hops 150
maximum transmission unit 503
Memory Buffer 453
MGMT port 33
MIB
and SNMP 460
supported MIBs 460
MIB (Management Information Base) 460
mini GBIC ports 32
connection speed 32
connector type 32
transceiver installation 32
transceiver removal 33
mirroring ports 162
monitor port 165, 166
MSA (MultiSource Agreement) 32
MST Instance, See MSTI 136
MST region 135
MSTI 136
MST ID 136
MSTI (Multiple Spanning Tree Instance) 134
MSTP 132, 134
bridge ID 155
configuration 147, 151
configuration digest 155
forwarding delay 150
Hello Time 155
hello time 149
Max Age 155
max age 150
max hops 150
MST region 135
network example 134
path cost 151
port priority 151
revision level 150
MSTP (Multiple Spanning Tree Protocol) 132
MTU 503
MTU (Multi-Tenant Unit) 63
multicast 227
802.1 priority 231, 237, 238, 241, 242
and IGMP 227
IGMP throttling 233
IP addresses 227
overview 227
setup 230, 231, 237, 238, 239, 241, 242
multicast group 235
multicast VLAN 248
Multiple Spanning Tree Instance, See MSTI 134

Multiple Spanning Tree Protocol 133
Multiple Spanning Tree Protocol, See MSTP. 132
Multiple STP 133
Multiple STP, see MSTP 134
MVR 244
  configuration 246
  group configuration 248
  network example 244
MVR (Multicast VLAN Registration) 244

N

network management system (NMS) 459
NTP (RFC-1305) 62

O

OAM 381
  details 383
  discovery 381
  port configuration 381
  remote loopback 381
  remote-loopback 389
Operations, Administration and Maintenance 381
other documentation 2

P

PAGP 310
password 42
  administrator 471
Path MTU 503
Path MTU Discovery 503
PHB (Per-Hop Behavior) 404
ping, test connection 483
policy 211, 402
  and classifier 211, 402
  and DiffServ 210
  configuration 211, 402
  example 213
  overview 210
  rules 210
policy routing
  benefits 400
  cost savings 400
  load sharing 400
  overview 400
policy-based routing 400
Port Aggregation Protocol, see PAgP
port authentication 185
  and RADIUS 254
  IEEE802.1x 187, 192, 256
  MAC authentication 186
port based VLAN type 64
port cloning 504, 506
  advanced settings 504, 506
  basic settings 504, 506
port details 52
port isolation 120
port mirroring 162, 166
  direction 166, 170
  egress 166, 170
  ingress 166, 170
port redundancy 175
port security 195, 199
  address learning 197
  limit MAC address learning 197
  MAC address learning 195, 199
  overview 195, 199
  setup 195, 199, 301, 308
port setup 69
port status 51
  port details 52
port VLAN trunking 103
port-based VLAN 117
  all connected 120
  port isolation 120
  settings wizard 120
ports
  “standby” 175
  diagnostics 483
  mirroring 162
  speed/duplex 72
power
  voltage 59, 61
power module
  disconnecting 34
power status 59, 61
PPPoE IA

trusted ports 318
untrusted ports 318
priority level 65
priority, queue assignment 65
product registration 537
protocol based VLAN 114
and IEEE 802.1Q tagging 114
example 116
hexadecimal notation for protocols 113, 115
isolate traffic 114
priority 113, 115
PVID 101, 111
PVID (Priority Frame) 101

Q

QoS
and classifier 201
queue weight 216
queuing 215
SPQ 216
WFQ 216
WRR 216
queuing method 215, 217

R

RADIUS 254
advantages 254
and authentication 254
Network example 253
server 254
settings 254
setup 254
Rapid Spanning Tree Protocol, See RSTP. 132
reboot
load configuration 452
reboot system 452
reflector port 162
registration
product 537
related documentation 2
remote management 480
service 481
trusted computers 481
remote port mirroring 162, 167
Removing the Fan Module 34
resetting 44, 451, 452, 453
to factory default settings 451, 452, 453
restoring configuration 44, 450
RFC 3164 486
RMirror 162
monitor port 168
reflector port 168
source 168
RMirror, see also remote port mirroring 167
Round Robin Scheduling 216
routing domain 65, 431
routing table 502
RSTP 132
rubber feet 26

S

save configuration 43, 452
Secure Shell See SSH
service access control 479
service port 480
sFlow 312
collector 314
configuration 312
datagram 312
overview 312
poll interval 314
sample rate 314
UDP port 315
sFlow agent 312
sFlow collector 312
Simple Network Management Protocol, see SNMP
SNMP 25, 459
agent 459
and MIB 460
authentication 470
communities 466
management model 459
manager 459
MIB 460
network components 459
object variables 460

protocol operations 460
security 470
setup 465
traps 466
users 469
version 3 and security 460
versions supported 459
SNMP traps 461
supported 461, 463, 465
source-based routing 400
Spanning Tree Protocol, See STP. 132
SPQ (Strict Priority Queuing) 216
SSH
encryption methods 474
how it works 473
implementation 474
SSH (Secure Shell) 472
SSL (Secure Socket Layer) 474
standby ports 175
static bindings 265
static MAC address 124
static MAC forwarding 112, 114, 124
static multicast address 127
static multicast forwarding 127
static route
overview 396
static routes 398
static trunking example 183
Static VLAN 107
static VLAN
control 109
tagging 109
status
LED 35
link aggregation 177
port 51
power 59, 61
STP 141, 145, 154
VLAN 104
VRRP 431
STP 132, 310
bridge ID 141, 146
bridge priority 139, 144
configuration 138, 142, 147
designated bridge 133
forwarding delay 140, 144
Hello BPDU 133
Hello Time 139, 141, 144, 146
how it works 133
Max Age 140, 141, 144, 146
path cost 132, 140, 145
port priority 140, 145
port state 133
root port 133
status 141, 145, 154
terminology 132
vs loop guard 299
subnet based VLANs 111
and DHCP VLAN 113
and priority 112
configuration 112
switch lockout 43
switch reset 44
switch setup 63
syslog 298, 486
protocol 486
settings 486
setup 486
severity levels 486
system information 56
system reboot 452

T

TACACS+ 254
setup 256
TACACS+ (Terminal Access Controller Access-Control System Plus) 253
tagged VLAN 101
Tech-Support 453
temperature indicator 58, 59, 60
time
current 62
time zone 62
Time (RFC-868) 62
time server 62
time service protocol 62
format 62
trademarks 537
transceiver
installation 32
removal 33

traps
destination 466
TRTCM
and bandwidth control 408
and DiffServ 410
color-aware mode 406
color-blind mode 406
setup 408
trunk group 175
trunking 175
example 183
trusted ports
ARP inspection 298
DHCP snooping 295
PPPoE IA 318
Tunnel Protocol Attribute, and RADIUS 261
Two Rate Three Color Marker (TRTCM) 405
Two Rate Three Color Marker, see TRTCM 405
Type of Service (ToS) 404

U

UDLD 310
UniDirectional Link Detection, see UDLD
untrusted ports
ARP inspection 298
DHCP snooping 295
PPPoE IA 318
user profiles 253

V

Vendor Specific Attribute See VSA
ventilation holes 26
VID 69, 101, 104, 105, 221
number of possible VIDs 101
priority frame 101
VID (VLAN Identifier) 101
Virtual Router
status 431
Virtual Router (VR) 430
Virtual Router Redundancy Protocol (VRRP) 430
VLAN 63, 101
acceptable frame type 111
automatic registration 102
ID 101
ingress filtering 111
introduction 63
number of VLANs 104
port number 105
port settings 109
port-based VLAN 117
port-based, all connected 120
port-based, isolation 120
port-based, wizard 120
static VLAN 107
status 104, 105
tagged 101
trunking 103, 111
type 64, 103
VLAN (Virtual Local Area Network) 63
VLAN mapping 303
activating 303
configuration 305
example 303
priority level 303
tagged 303
traffic flow 303
untagged 303
VLAN ID 303
VLAN number 66, 67, 69
VLAN stacking 219, 221
configuration 221
example 219
frame format 221
port roles 220, 223
port-based Q-in-Q 223
priority 221
selective Q-in-Q 225
VLAN Trunking Protocol, see VTP
VLAN, protocol based, See protocol based VLAN
VLAN, subnet based, See subnet based VLANs 111
VRID (Virtual Router ID) 431
VRRP 430
advertisement interval 433
authentication 432
backup router 430
configuration example 435
Hello message 433
how it works 430
interface setup 431

master router 430
network example 430, 435
parameters 433
preempt mode 433, 434
priority 433, 434
status 431
uplink gateway 434
uplink status 431
Virtual Router 430
Virtual Router ID 434
VRID 431
VSA 260
VTP 310

W

warranty 537
note 537
web configurator 25, 37
getting help 45
layout 38
login 37
logout 45
navigation panel 39
weight, queuing 216
Weighted Round Robin Scheduling (WRR) 216
WFQ (Weighted Fair Queuing) 216
WRR (Weighted Round Robin Scheduling 216

Z

ZON Neighbor Management 49
ZON Utility 49
ZULD 390
example 390
probe time 393
status 391
ZULD (ZyXEL Unidirectional Link Detection) 390
ZyNOS (ZyXEL Network Operating System) 455
ZyXEL Unidirectional Link Detection 390
ZyXEL Unidirectional Link Detection (ZULD) 390