ZYXEL
Your Networking Ally

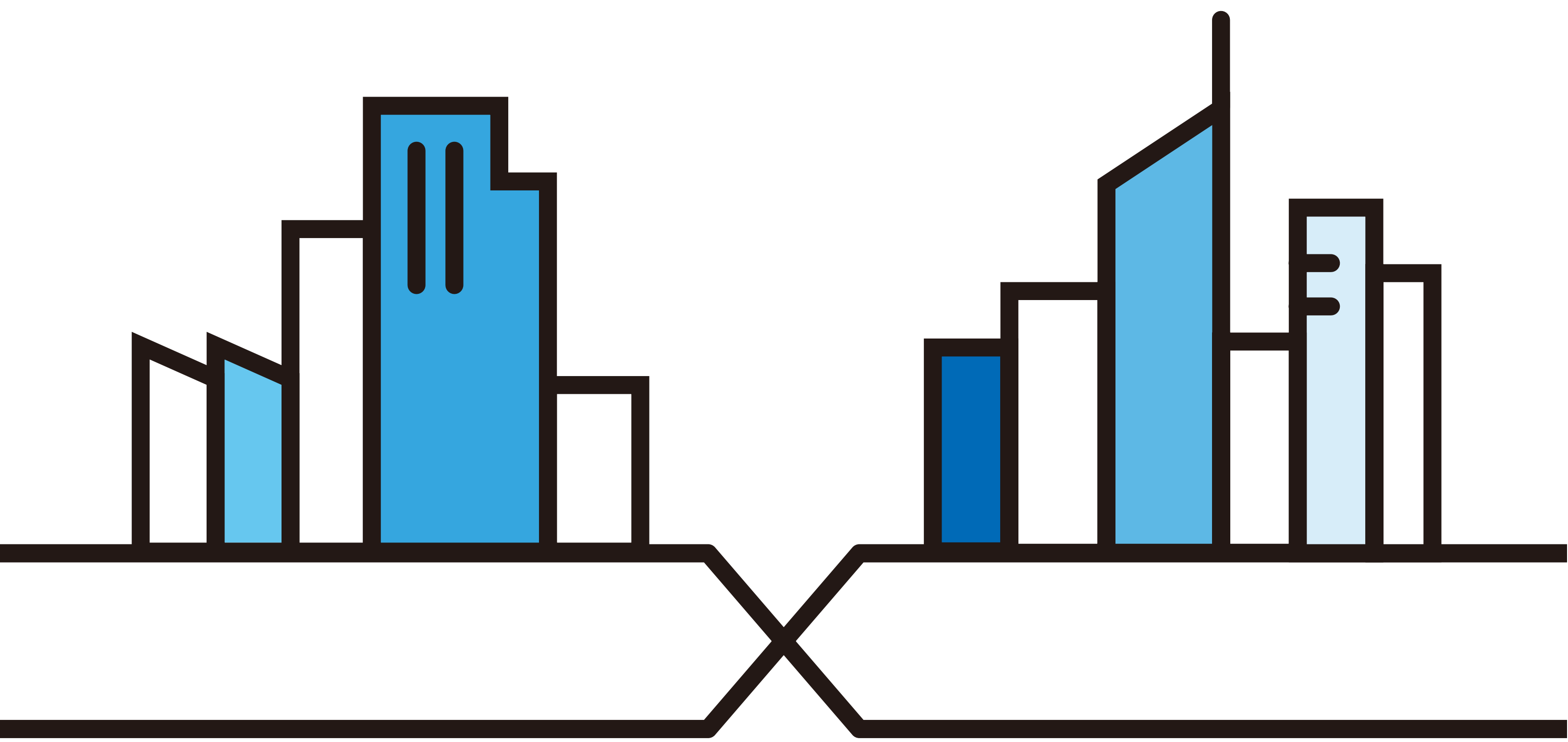
User's Guide

GS2220 Series

8/24/44-Port GbE L2 Switch with 2/4 Dual Personality GbE Uplinks
8/24/44-Port GbE L2 PoE Switch with 2/4 Dual Personality GbE Uplinks

Version 4.70 Edition 1, 07/2020

Default Login Details	
Management IP Address	http://DHCP-assigned IP or http://192.168.1.1
User Name	admin
Password	1234



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- 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 **https://businessforum.zyxel.com** for product discussions.

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

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.

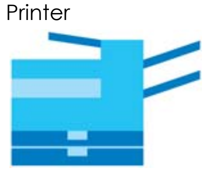
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- All models may be referred to as the "Switch" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Basic Setting** > **IP Setup** > **IP Configuration** > **Network Proxy Configuration** means you first click **Basic Setting** in the navigation panel, then the **IP Setup** sub menu, then **IP Configuration** and finally **Network Proxy Configuration** to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The Switch icon is not an exact representation of your device.

Switch 	Generic Router 	Wireless Router / Access Point 
Generic Switch 	Smart TV 	Desktop 
Laptop 	IP Camera 	Printer 
Server 		

Contents Overview

User's Guide 23

Getting to Know Your Switch 24
Hardware Installation and Connection 33
Hardware Panels 39

Technical Reference 49

Web Configurator 50
Initial Setup Example 78
Tutorials 83
Status 94
Basic Setting 100
VLAN 133
Static MAC Forwarding 154
Static Multicast Forwarding 156
Filtering 160
Spanning Tree Protocol 162
Bandwidth Control 183
Broadcast Storm Control 185
Mirroring 187
Link Aggregation 189
Port Authentication 196
Port Security 205
Time Range 207
Classifier 209
Policy Rule 218
Queuing Method 222
Multicast 225
AAA 248
IP Source Guard 260
DHCP Snooping 266
ARP Inspection 276
Loop Guard 292
VLAN Mapping 295
Layer 2 Protocol Tunneling 299
PPPoE 303
Error Disable 311
VLAN Isolation 318
Green Ethernet 320

Link Layer Discovery Protocol (LLDP) 322
Anti-Arpscan 344
BPDU Guard 349
OAM 352
ZULD 359
Auto PD Recovery 363
Static Route 368
Differentiated Services 371
DHCP 375
ARP Setup 388
Maintenance 392
Access Control 406
Diagnostic 430
System Log 433
Syslog Setup 434
Cluster Management 437
MAC Table 443
ARP Table 446
Path MTU Table 448
Configure Clone 449
IPv6 Neighbor Table 452
Port Status 454
Networked AV Mode 461
System 464
Port 469
Switching 476
Networking 499
Security 501
Maintenance 512

Troubleshooting and Appendices 519

Troubleshooting 520

Table of Contents

Document Conventions 3

Contents Overview 4

Table of Contents 6

Part I: User's Guide 23

Chapter 1
Getting to Know Your Switch 24

1.1 Introduction 24
1.1.1 Management Method 25
1.1.2 Management Modes 25
1.1.3 Mode Changing 25
1.1.4 ZON Utility 27
1.1.5 Web Configurator Networked AV Mode 27
1.1.6 PoE 27
1.2 Example Applications 27
1.2.1 PoE Example Application 28
1.2.2 Backbone Example Application 28
1.2.3 Bridging or Fiber Uplink Example Application 29
1.2.4 High Performance Switching Example 30
1.2.5 IEEE 802.1Q VLAN Application Examples 30
1.2.6 IPv6 Support 31
1.3 Ways to Manage the Switch 31
1.4 Good Habits for Managing the Switch 32

Chapter 2
Hardware Installation and Connection 33

2.1 Installation Scenarios 33
2.2 Safety Precautions 33
2.3 Desktop Installation Procedure 33
2.4 Wall Mounting (GS2220-10 and GS2220-10HP Only) 34
2.4.1 Installation Requirements 34
2.5 Mounting the Switch on a Rack 36
2.5.1 Installation Requirements 36
2.5.2 Precautions 37
2.5.3 Attaching the Mounting Brackets to the Switch 37

2.5.4 Mounting the Switch on a Rack ... 37

Chapter 3
Hardware Panels ... 39

3.1 Front Panel Connections ... 39
3.1.1 Gigabit Ethernet Ports ... 40
3.1.2 PoE (GS2220-10HP, GS2220-28HP and GS2220-50HP) ... 41
3.1.3 SFP Slots ... 41
3.1.4 Dual Personality Interfaces ... 43
3.1.5 Console Port ... 44
3.2 Rear Panel ... 44
3.2.1 Grounding ... 45
3.2.2 AC Power Connection ... 46
3.3 LEDs ... 47

Part II: Technical Reference ... 49

Chapter 4
Web Configurator ... 50

4.1 Overview ... 50
4.2 System Login ... 50
4.3 Zyxel One Network (ZON) Utility ... 54
4.3.1 Requirements ... 54
4.3.2 Run the ZON Utility ... 55
4.4 Wizard ... 58
4.4.1 Basic Settings ... 59
4.4.2 Advanced Settings ... 63
4.5 Web Configurator Layout ... 68
4.5.1 Change Your Password ... 74
4.6 Save Your Configuration ... 75
4.7 Switch Lockout ... 75
4.8 Reset the Switch ... 76
4.8.1 Restore Button ... 76
4.8.2 Restore Custom Default ... 76
4.8.3 Reboot the Switch ... 76
4.9 Log Out of the Web Configurator ... 76
4.10 Help ... 77

Chapter 5
Initial Setup Example ... 78

5.1 Overview ... 78

5.1.1 Create a VLAN 78
5.1.2 Set Port VID 80
5.1.3 Configure Switch Management IP Address 81

Chapter 6
Tutorials 83

6.1 Overview 83
6.2 How to Use DHCPv4 Snooping on the Switch 83
6.3 How to Use DHCPv4 Relay on the Switch 87
6.3.1 DHCP Relay Tutorial Introduction 87
6.3.2 Create a VLAN 87
6.3.3 Configure DHCPv4 Relay 90
6.3.4 Troubleshooting 91
6.4 How to Use Auto Configuration via a DHCP Server on the Switch 91

Chapter 7
Status 94

7.1 Overview 94
7.1.1 What You Can Do 94
7.2 Status 94
7.2.1 Neighbor Screen 96
7.2.2 Neighbor Detail 98

Chapter 8
Basic Setting 100

8.1 Overview 100
8.1.1 What You Can Do 100
8.2 System Information 100
8.3 General Setup 102
8.4 Introduction to VLANs 104
8.5 Switch Setup 105
8.6 IP Setup 106
8.6.1 IP Status 106
8.6.2 IP Status Details 107
8.6.3 IP Configuration 108
8.6.4 Network Proxy Configuration 110
8.7 Port Setup 111
8.8 PoE Status 113
8.8.1 PoE Time Range Setup 115
8.8.2 PoE Setup 116
8.9 Interface Setup 119
8.10 IPv6 120
8.10.1 IPv6 Status 120

8.10.2 IPv6 Interface Status 120
8.10.3 IPv6 Configuration 123
8.10.4 IPv6 Global Setup 123
8.10.5 IPv6 Interface Setup 124
8.10.6 IPv6 Link-Local Address Setup 125
8.10.7 IPv6 Global Address Setup 126
8.10.8 IPv6 Neighbor Discovery Setup 127
8.10.9 IPv6 Neighbor Setup 128
8.10.10 DHCPv6 Client Setup 129
8.11 Cloud Management 131
8.11.1 Nebula Center Control Discovery 131
8.11.2 Nebula Switch Registration 132

Chapter 9
VLAN........133

9.1 Overview 133
9.1.1 What You Can Do 133
9.1.2 What You Need to Know 134
9.2 IEEE 802.1Q Tagged VLANs 134
9.3 VLAN Status 137
9.3.1 VLAN Details 138
9.4 VLAN Configuration 139
9.5 Configure a Static VLAN 139
9.6 Configure VLAN Port Settings 141
9.7 Subnet Based VLANs 142
9.7.1 Configuring Subnet Based VLAN 143
9.8 Protocol Based VLANs 145
9.8.1 Configuring Protocol Based VLAN 145
9.9 Voice VLAN 147
9.10 MAC Based VLAN 148
9.11 Vendor ID Based VLAN 149
9.12 Port-Based VLAN Setup 151
9.12.1 Configure a Port-Based VLAN 151

Chapter 10
Static MAC Forwarding........154

10.1 Overview 154
10.1.1 What You Can Do 154
10.2 Configure Static MAC Forwarding 154

Chapter 11
Static Multicast Forwarding........156

11.1 Overview 156

11.1.1 What You Can Do 156
11.1.2 What You Need To Know 156
11.2 Configure Static Multicast Forwarding 157

Chapter 12
Filtering 160

12.1 Filtering Overview 160
12.1.1 What You Can Do 160
12.2 Configure a Filtering Rule 160

Chapter 13
Spanning Tree Protocol 162

13.1 Spanning Tree Protocol Overview 162
13.1.1 What You Can Do 162
13.1.2 What You Need to Know 162
13.2 Spanning Tree Protocol Status 165
13.3 Spanning Tree Configuration 165
13.4 Rapid Spanning Tree Protocol Status 166
13.5 Configure Rapid Spanning Tree Protocol 168
13.6 Configure Multiple Spanning Tree Protocol 169
13.6.1 Multiple Spanning Tree Protocol Port Configuration 174
13.7 Multiple Spanning Tree Protocol Status 174
13.8 Configure Multiple Rapid Spanning Tree Protocol 177
13.9 Multiple Rapid Spanning Tree Protocol Status 179
13.10 Technical Reference 180
13.10.1 MSTP Network Example 181
13.10.2 MST Region 181
13.10.3 MST Instance 182
13.10.4 Common and Internal Spanning Tree (CIST) 182

Chapter 14
Bandwidth Control 183

14.1 Bandwidth Control Overview 183
14.1.1 What You Can Do 183
14.2 Bandwidth Control Setup 183

Chapter 15
Broadcast Storm Control 185

15.1 Broadcast Storm Control Overview 185
15.1.1 What You Can Do 185
15.2 Broadcast Storm Control Setup 185

Chapter 16
Mirroring 187

16.1 Mirroring Overview 187
16.2 Port Mirroring Setup 187

Chapter 17
Link Aggregation 189

17.1 Link Aggregation Overview 189
17.1.1 What You Can Do 189
17.1.2 What You Need to Know 189
17.2 Link Aggregation Status 190
17.3 Link Aggregation Setting 191
17.3.1 Link Aggregation Control Protocol 193
17.4 Technical Reference 194
17.4.1 Static Trunking Example 194

Chapter 18
Port Authentication 196

18.1 Port Authentication Overview 196
18.1.1 What You Can Do 196
18.1.2 What You Need to Know 197
18.1.3 MAC Authentication 197
18.2 Port Authentication Configuration 198
18.3 Activate IEEE 802.1x Security 198
18.4 Activate MAC Authentication 199
18.5 Guest VLAN 201
18.6 Compound Authentication 203

Chapter 19
Port Security 205

19.1 About Port Security 205
19.2 Port Security Setup 205

Chapter 20
Time Range 207

20.1 Time Range Overview 207
20.1.1 What You Can Do 207
20.2 Configuring Time Range 207

Chapter 21
Classifier 209

21.1 Classifier Overview 209
21.1.1 What You Can Do 209
21.1.2 What You Need to Know 209
21.2 Classifier Status 210

21.3 Classifier Configuration 210
21.3.1 Viewing and Editing Classifier Configuration Summary 214
21.4 Classifier Global Setting Configuration 215
21.5 Classifier Example 216

Chapter 22
Policy Rule 218

22.1 Policy Rules Overview 218
22.1.1 What You Can Do 218
22.1.2 DiffServ 218
22.1.3 DSCP and Per-Hop Behavior 218
22.2 Configuring Policy Rules 219
22.3 Policy Example 221

Chapter 23
Queuing Method 222

23.1 Queuing Method Overview 222
23.1.1 What You Can Do 222
23.1.2 What You Need to Know 222
23.2 Configuring Queuing 223

Chapter 24
Multicast 225

24.1 Multicast Overview 225
24.1.1 What You Can Do 225
24.1.2 What You Need to Know 225
24.2 Multicast Setup 229
24.3 IPv4 Multicast Status 229
24.3.1 IGMP Snooping 230
24.3.2 IGMP Snooping VLAN 233
24.3.3 IGMP Filtering Profile 234
24.4 IPv6 Multicast Status 236
24.4.1 MLD Snooping-proxy 236
24.4.2 MLD Snooping-proxy VLAN 237
24.4.3 MLD Snooping-proxy VLAN Port Role Setting 238
24.4.4 MLD Snooping-proxy Filtering 240
24.4.5 MLD Snooping-proxy Filtering Profile 241
24.5 General MVR Configuration 242
24.5.1 MVR Group Configuration 244
24.5.2 MVR Configuration Example 246

Chapter 25
AAA 248

25.1 Authentication, Authorization and Accounting (AAA) 248
25.1.1 What You Can Do 248
25.1.2 What You Need to Know 248
25.2 AAA Screens 249
25.3 RADIUS Server Setup 249
25.4 TACACS+ Server Setup 251
25.5 AAA Setup 253
25.6 Technical Reference 255
25.6.1 Vendor Specific Attribute 255
25.6.2 Supported RADIUS Attributes 257
25.6.3 Attributes Used for Authentication 257
25.6.4 Attributes Used for Accounting 258

Chapter 26
IP Source Guard 260

26.1 IP Source Guard Overview 260
26.1.1 What You Can Do 260
26.1.2 What You Need to Know 261
26.2 IP Source Guard 262
26.3 IPv4 Source Guard Setup 262
26.4 IPv4 Source Guard Static Binding 263

Chapter 27
DHCP Snooping 266

27.1 DHCP Snooping Overview 266
27.2 DHCP Snooping 266
27.3 DHCP Snooping Configure 269
27.3.1 DHCP Snooping Port Configure 270
27.3.2 DHCP Snooping VLAN Configure 271
27.3.3 DHCP Snooping VLAN Port Configure 272
27.4 Technical Reference 273
27.4.1 DHCP Snooping Overview 274

Chapter 28
ARP Inspection 276

28.1 ARP Inspection Status 276
28.1.1 ARP Inspection VLAN Status 277
28.1.2 ARP Inspection Log Status 277
28.2 ARP Inspection Configure 278
28.2.1 ARP Inspection Port Configure 280
28.2.2 ARP Inspection VLAN Configure 281
28.3 IPv6 Source Guard Overview 282
28.4 IPv6 Source Binding Status 282

28.5 IPv6 Static Binding Setup 283
28.6 IPv6 Source Guard Policy Setup 285
28.7 IPv6 Source Guard Port Setup 286
28.8 IPv6 Snooping Policy Setup 286
28.9 IPv6 Snooping VLAN Setup 287
28.10 IPv6 DHCP Trust Setup 288
28.11 Technical Reference 289
28.11.1 ARP Inspection Overview 290

Chapter 29
Loop Guard 292

29.1 Loop Guard Overview 292
29.1.1 What You Can Do 292
29.1.2 What You Need to Know 292
29.2 Loop Guard Setup 294

Chapter 30
VLAN Mapping 295

30.1 VLAN Mapping Overview 295
30.1.1 VLAN Mapping Example 295
30.1.2 What You Can Do 295
30.2 Enable VLAN Mapping 296
30.2.1 VLAN Mapping Configure 296

Chapter 31
Layer 2 Protocol Tunneling 299

31.1 Layer 2 Protocol Tunneling Overview 299
31.1.1 What You Can Do 299
31.1.2 What You Need to Know 299
31.2 Configuring Layer 2 Protocol Tunneling 300

Chapter 32
PPPoE 303

32.1 PPPoE Intermediate Agent Overview 303
32.1.1 What You Can Do 303
32.1.2 What You Need to Know 303
32.2 PPPoE 305
32.3 PPPoE Intermediate Agent 306
32.3.1 PPPoE IA Per-Port 307
32.3.2 PPPoE IA Per-Port Per-VLAN 308
32.3.3 PPPoE IA for VLAN 309

Chapter 33
Error Disable 311

33.1 Error Disable Overview 311
33.1.1 CPU Protection Overview 311
33.1.2 Error-Disable Recovery Overview 311
33.1.3 What You Can Do 311
33.2 Error Disable Settings 312
33.3 Error-Disable Status 312
33.4 CPU Protection Configuration 314
33.5 Error-Disable Detect Configuration 315
33.6 Error-Disable Recovery Configuration 316

Chapter 34
VLAN Isolation 318

34.1 VLAN Isolation Overview 318
34.2 Configuring VLAN Isolation 318

Chapter 35
Green Ethernet 320

35.1 Green Ethernet Overview 320
35.2 Configuring Green Ethernet 320

Chapter 36
Link Layer Discovery Protocol (LLDP) 322

36.1 LLDP Overview 322
36.2 LLDP-MED Overview 323
36.3 LLDP Settings 324
36.4 LLDP Local Status 325
36.4.1 LLDP Local Port Status Detail 326
36.5 LLDP Remote Status 329
36.5.1 LLDP Remote Port Status Detail 330
36.6 LLDP Configuration 336
36.6.1 LLDP Configuration Basic TLV Setting 337
36.6.2 LLDP Configuration Org-specific TLV Setting 338
36.7 LLDP-MED Configuration 339
36.8 LLDP-MED Network Policy 340
36.9 LLDP-MED Location 341

Chapter 37
Anti-Arpscan 344

37.1 Anti-Arpscan Overview 344
37.1.1 What You Can Do 344
37.1.2 What You Need to Know 344
37.2 Anti-Arpscan Status 345
37.3 Anti-Arpscan Host Status 345

37.4 Anti-Arpscan Trust Host 346
37.5 Anti-Arpscan Configure 347

Chapter 38
BPDU Guard 349

38.1 BPDU Guard Overview 349
38.1.1 What You Can Do 349
38.2 BPDU Guard Status 349
38.3 BPDU Guard Configuration 350

Chapter 39
OAM 352

39.1 OAM Overview 352
39.1.1 What You Can Do 352
39.2 OAM Status 352
39.2.1 OAM Details 353
39.3 OAM Configuration 356
39.4 OAM Remote Loopback 357

Chapter 40
ZULD 359

40.1 ZULD Overview 359
40.1.1 What You Can Do 359
40.1.2 What You Need to Know 359
40.2 ZULD Status 360
40.3 ZULD Configuration 361

Chapter 41
Auto PD Recovery 363

41.1 Auto PD Recovery Overview 363
41.1.1 What You Can Do 363
41.2 Auto PD Recovery 363
41.2.1 Activate the Automatic PD Recovery 365

Chapter 42
Static Route 368

42.1 Static Routing 368
42.1.1 What You Can Do 368
42.2 Static Routing 369
42.3 IPv4 Static Route 369

Chapter 43
Differentiated Services 371

43.1 DiffServ Overview 371
43.1.1 What You Can Do 371
43.1.2 What You Need to Know 371
43.2 Activating DiffServ 372
43.3 DSCP-to-IEEE 802.1p Priority Settings 373
43.3.1 Configuring DSCP Settings 373

Chapter 44
DHCP 375

44.1 DHCP Overview 375
44.1.1 What You Can Do 375
44.1.2 What You Need to Know 375
44.2 DHCP Configuration 376
44.3 DHCPv4 Status 376
44.4 DHCPv4 Relay 377
44.4.1 DHCPv4 Relay Agent Information 377
44.4.2 DHCPv4 Option 82 Profile 378
44.4.3 Configuring DHCPv4 Global Relay 379
44.4.4 Configure DHCPv4 Global Relay Port 380
44.4.5 Global DHCP Relay Configuration Example 381
44.4.6 DHCPv4 VLAN Setting 382
44.4.7 Configure DHCPv4 VLAN Port 383
44.4.8 Example: DHCP Relay for Two VLANs 384
44.5 DHCPv6 Relay 385
44.6 DHCP Server Guard 387

Chapter 45
ARP Setup 388

45.1 ARP Overview 388
45.1.1 What You Can Do 388
45.1.2 What You Need to Know 388
45.2 ARP Setup 390
45.2.1 ARP Learning 390

Chapter 46
Maintenance 392

46.1 Overview 392
46.1.1 What You Can Do 392
46.2 Maintenance Settings 392
46.2.1 Erase Running-Configuration 394
46.2.2 Save Configuration 394
46.2.3 Reboot System 394
46.2.4 Factory Default 395

46.2.5 Custom Default 395
46.3 Firmware Upgrade 396
46.4 Restore Configuration 397
46.5 Backup Configuration 398
46.6 Auto Configuration 398
46.7 Tech-Support 399
46.7.1 Tech-Support Download 401
46.8 Certificates 401
46.8.1 HTTPS Certificates 402
46.9 Technical Reference 403
46.9.1 FTP Command Line 403
46.9.2 Filename Conventions 403
46.9.3 FTP Command Line Procedure 404
46.9.4 GUI-based FTP Clients 405
46.9.5 FTP Restrictions 405

Chapter 47
Access Control........406

47.1 Access Control Overview 406
47.1.1 What You Can Do 406
47.2 Access Control Main Settings 406
47.3 Configure SNMP 407
47.3.1 Configure SNMP Trap Group 408
47.3.2 Enable or Disable Sending of SNMP Traps on a Port 409
47.3.3 Configure SNMP User 410
47.4 Set Up Login Accounts 412
47.5 Service Access Control 414
47.6 Remote Management 415
47.7 Technical Reference 416
47.7.1 About SNMP 416
47.7.2 SSH Overview 422
47.7.3 Introduction to HTTPS 424
47.7.4 Google Chrome Warning Messages 428

Chapter 48
Diagnostic........430

48.1 Overview 430
48.2 Diagnostic 430

Chapter 49
System Log........433

49.1 Overview 433
49.2 System Log 433

Chapter 50
Syslog Setup 434

50.1 Syslog Overview 434
50.1.1 What You Can Do 434
50.2 Syslog Setup 434

Chapter 51
Cluster Management...437

51.1 Cluster Management Overview 437
51.1.1 What You Can Do 438
51.2 Cluster Management Status 438
51.3 Clustering Management Configuration 439
51.4 Technical Reference 440
51.4.1 Cluster Member Switch Management 441

Chapter 52
MAC Table 443

52.1 MAC Table Overview 443
52.1.1 What You Can Do 443
52.1.2 What You Need to Know 443
52.2 Viewing the MAC Table 444

Chapter 53
ARP Table 446

53.1 Overview 446
53.1.1 What You Can Do 446
53.1.2 What You Need to Know 446
53.2 Viewing the ARP Table 446

Chapter 54
Path MTU Table 448

54.1 Path MTU Overview 448
54.2 Viewing the Path MTU Table 448

Chapter 55
Configure Clone...449

55.1 Overview 449
55.2 Configure Clone 449

Chapter 56
IPv6 Neighbor Table...452

56.1 IPv6 Neighbor Table Overview 452
56.2 Viewing the IPv6 Neighbor Table 452

Chapter 57
Port Status 454

57.1 Overview 454
57.2 Port Status 454
57.2.1 Port Details 455
57.2.2 DDMI 458
57.2.3 DDMI Details 458
57.2.4 Port Utilization 460

Chapter 58
Networked AV Mode...461

58.1 Overview 461
58.2 Summary 461

Chapter 59
System...464

59.1 What You Can Do 464
59.2 System Information 464
59.3 General Setup 465
59.4 Cloud Management 467

Chapter 60
Port 469

60.1 What You Can Do 469
60.2 PoE Status 469
60.3 PoE Setup 471
60.4 Port Setup 473

Chapter 61
Switching..476

61.1 Broadcast Storm Control 476
61.2 Link Aggregation 477
61.2.1 What You Can Do 477
61.3 Link Aggregation Status 477
61.4 Link Aggregation Setting 478
61.5 Link Aggregation Control Protocol 480
61.6 VLAN 482
61.6.1 What You Can Do 482
61.6.2 What You Need to Know 482
61.7 VLAN Status 485
61.7.1 VLAN Detail 485
61.8 Static VLAN 486
61.9 VLAN Port Setting 488

61.10 Multicast 490
61.10.1 What You Can Do 490
61.11 IPv4 Multicast Status 490
61.12 IGMP Snooping 491
61.13 IGMP Snooping VLAN 494
61.14 IGMP Filtering Profile 496

Chapter 62
Networking 499

62.1 IP Setup 499

Chapter 63
Security 501

63.1 Access Control 501
63.1.1 What You Can Do 501
63.2 Set Up Login Accounts 501
63.3 Remote Management 503
63.4 Configure SNMP 504
63.5 Configure SNMP Trap Group 506
63.6 Enable or Disable Sending of SNMP Traps on a Port 507
63.7 Configure SNMP User 509
63.8 Service Access Control 510

Chapter 64
Maintenance 512

64.1 What You Can Do 512
64.2 Backup Configuration 512
64.3 Firmware Upgrade 513
64.4 Reboot System 514
64.5 Restore Configuration 515
64.6 Save Configuration 515
64.7 Tech-Support 516
64.8 Port Mirroring 517

Part III: Troubleshooting and Appendices 519

Chapter 65
Troubleshooting 520

65.1 Power, Hardware Connections, and LEDs 520
65.2 Switch Access and Login 521
65.3 Switch Configuration 522

Appendix A Customer Support 524

Appendix B Common Services 530

Appendix C IPv6 533

Appendix D Legal Information 541

Index 546

PART I
User's Guide

CHAPTER 1
Getting to Know Your Switch

1.1 Introduction

The GS2220 Series consists of the following models:

- GS2220-10
- GS2220-10HP
- GS2220-28
- GS2220-28HP
- GS2220-50
- GS2220-50HP

References to PoE models in this User's Guide only apply to GS2220-10HP, GS2220-28HP and GS2220-50HP.

The Switch is a layer-2 Ethernet switch that only does switching.

The Switch supports NebulaFlex which can set the Switch to operate in either standalone or Nebula cloud management mode. When the Switch is in standalone mode, it can be configured and managed by the Web Configurator, via Telnet, any terminal emulator program using the Command Line Interface (CLI), or via third-party SNMP management. When the Switch is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control Center (NCC) (see Section 8.11 on page 131).

All models are referred to as the "Switch" in this guide.

The following table describes the hardware features of the Switch by model.

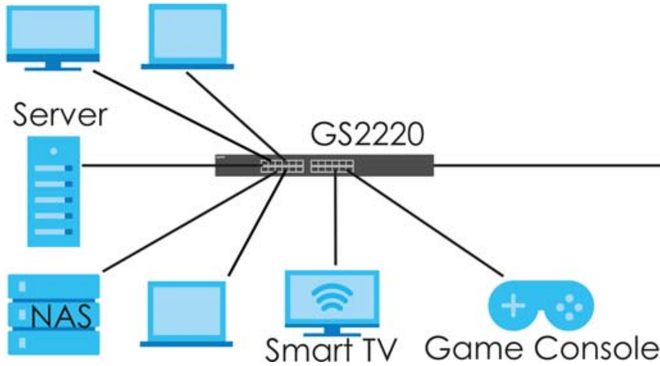
Table 1 GS2220 Series Comparison Table

FEATURE	GS2220-10	GS2220-10HP	GS2220-28	GS2220-28HP	GS2220-50	GS2220-50HP
10/100/1000 Mbps Ethernet ports	8	0	24	0	44	0
10/100/1000 Mbps PoE ports	0	8	0	24	0	48
GbE combo ports (dual personality interfaces)	2	2	4	4	4	4
1 Gbps SFP interfaces	0	0	0	0	2	2
Fan	0	1	0	2	1	2
Rubber feet for desktop placement	Yes	Yes	Yes	Yes	Yes	Yes

Table 1 GS2220 Series Comparison Table

FEATURE	GS2220-10	GS2220-10HP	GS2220-28	GS2220-28HP	GS2220-50	GS2220-50HP
Wall-mount	Yes	Yes	No	No	No	No
Rack-mount	Yes	Yes	Yes	Yes	Yes	Yes

Figure 1 GS2220 Series Switch Application



1.1.1 Management Method

With its built-in Web Configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program using the Command Line Interface (CLI), or third-party SNMP management.

1.1.2 Management Modes

NebulaFlex means you can set the Switch to operate in either standalone or cloud mode (but not both at the same time).

Use the Web Configurator to configure and manage the Switch directly in standalone mode or use Nebula Control Center (NCC) to configure and manage the Switch in cloud mode. The Nebula Control

Center (NCC) is an alternative cloud-based network management system that allows you to remotely manage and monitor the Switch. You may also access a minimized version of the Web Configurator in cloud mode.

Nebula Cloud Management

To have Nebula manage the Switch, you must first register it at the Nebula web portal at https://nebula.zyxel.com, and ensure that **Nebula Control Center Discovery** is enabled in **Basic Setting** > **Cloud Management** > **Nebula Control Center Discovery** in the Switch Web Configurator.

Note: See the Switch's datasheet for the feature differences between standalone and Nebula cloud management modes. You can find the Switch's datasheet at the Zyxel website.

See the NCC (Nebula Control Center) User's Guide for how to configure the Switch using Nebula.

1.1.3 Mode Changing

This section describes how to change the Switch's management mode.

Note: If you change the Switch's management mode from standalone mode to Nebula-managed mode, the configuration settings of the Switch will be overwritten with what you have configured in Nebula.

Note: If you change the Switch's management mode from Nebula-managed mode to standalone mode, the Switch will reset to its factory-default settings.

From Standalone to Nebula Cloud Management

To manage your Switch via Nebula, connect the Switch to the Internet, and register it to a site and organization at the Nebula web portal (https://nebula.zyxel.com).

See the following steps or the Switch Quick Start Guide for how to do device registration.

Go to the NCC to Register the Switch

1 Go to the Nebula web portal in one of three ways.

- Type https://nebula.zyxel.com in a supported web browser. See the Nebula User's Guide for more information about supported browsers.
- Click **Visit Nebula** in the Switch's login page.
- Click the **Nebula** icon in the upper right corner of the Switch's Web Configurator.

2 Click **Login** in the Nebula web portal. Enter your myZyxel account information. You will be redirected to another screen where you can sign up for a myZyxel account if you do not have one.

3 Create an organization and a site or select an existing site using the Nebula setup wizard.

4 Register the Switch by entering its MAC address and serial number and assign it to the site. The serial number and MAC address can be found in the **Status** screen or the device back label on the Switch.

Use the Zyxel Nebula Mobile App to Register the Switch

1 Download and open the Zyxel Nebula Mobile app in your mobile device. Click **Sign Up** to create a myZyxel account or enter your existing account information to log in.

2 Create an organization and site, or select an existing site using the Zyxel Nebula Mobile app.

3 Select a site and scan the Switch's QR code to add it to the site. You can find the QR code:

- On a label on the Switch or
- On its box or
- In the Web Configurator at **Basic** > **Cloud Management** > **Nebula Switch Registration**.

See Section 3.3 on page 47 for more information about the **CLOUD** LED or Section 7.2 on page 94 for more information about the **Hybrid Mode** field in the **Status** screen to see if the Switch goes into Nebula cloud management mode successfully.

Note: The Switch goes into Nebula-managed mode automatically after it can access the Nebula web portal and is successfully registered there. Its login password and settings are then overwritten with what you have configured in the Nebula web portal.

From Nebula-managed to Standalone

To return to direct management standalone mode, just remove (unregister) the Switch from the organization or site in the Nebula web portal. The Switch will reboot and restore the factory default settings.

1.1.4 ZON Utility

With its built-in Web Configurator, including the Neighbor Management feature (Section 7.2.1 on page 96), viewing, managing and configuring the Switch and its neighboring devices is easy.

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 (Windows operation system). For more information on ZON Utility see Section 4.3 on page 54.

1.1.5 Web Configurator Networked AV Mode

Aside from the Web Configurator in Standard mode, you can switch to Networked AV mode that is specifically designed to simplify configuration and management of the Switch for AVoIP (Audio-Video over Internet Protocol) application. AV over IP is the transmission of audio-video data over a network.

1.1.6 PoE

The Switch is a Power Sourcing Equipment (PSE) because it provides a source of power via its Ethernet ports. Each device that receives power through an Ethernet port is a Powered Device (PD).

The Switch can adjust the power supplied to each PD according to the PoE standard the PD supports. PoE standards are:

- IEEE 802.3af Power over Ethernet (PoE)
- IEEE 802.3at Power over Ethernet (PoE) Plus

The following table describes the PoE features of the Switch by model.

Table 2 GS2220 Series Models and PoE Features

POE FEATURES	GS2220-10HP	GS2220-28HP	GS2220-50HP
IEEE 802.3af PoE	Yes	Yes	Yes
IEEE 802.3at PoE Plus	Yes	Yes	Yes
Power Management Mode	Consumption Classification (default)	Consumption Classification (default)	Consumption Classification (default)
PoE Power Budget	180 W	375 W	375 W

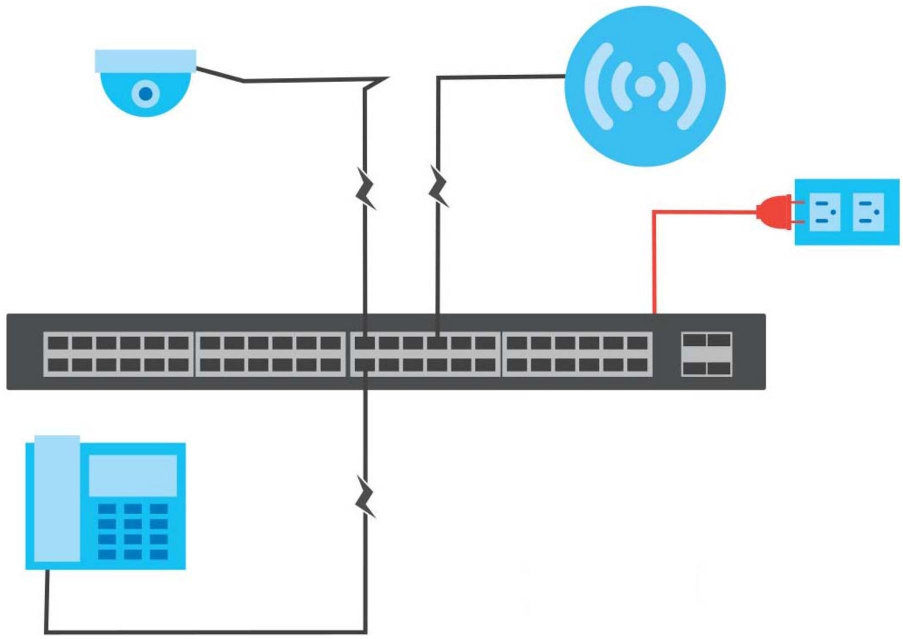
1.2 Example Applications

This section shows a few examples of using the Switch in various network environments. Note that the Switch in the figure is just an example Switch and not your actual Switch.

1.2.1 PoE Example Application

The following example figure shows a Switch supplying PoE (Power over Ethernet) to Powered Devices (PDs) such as an IP camera, a wireless router, an IP telephone and a general outdoor router that are not within reach of a power outlet.

Figure 2 PoE Example Application

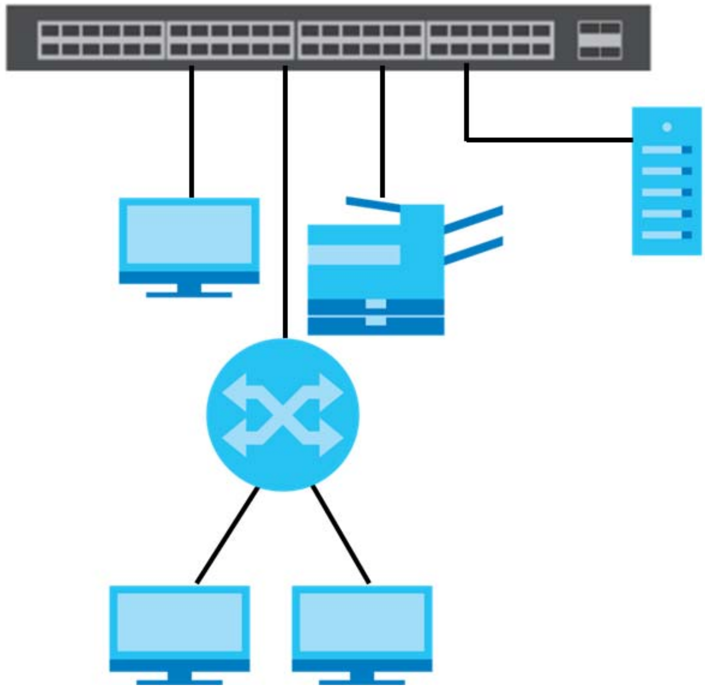


1.2.2 Backbone Example Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone 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.

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

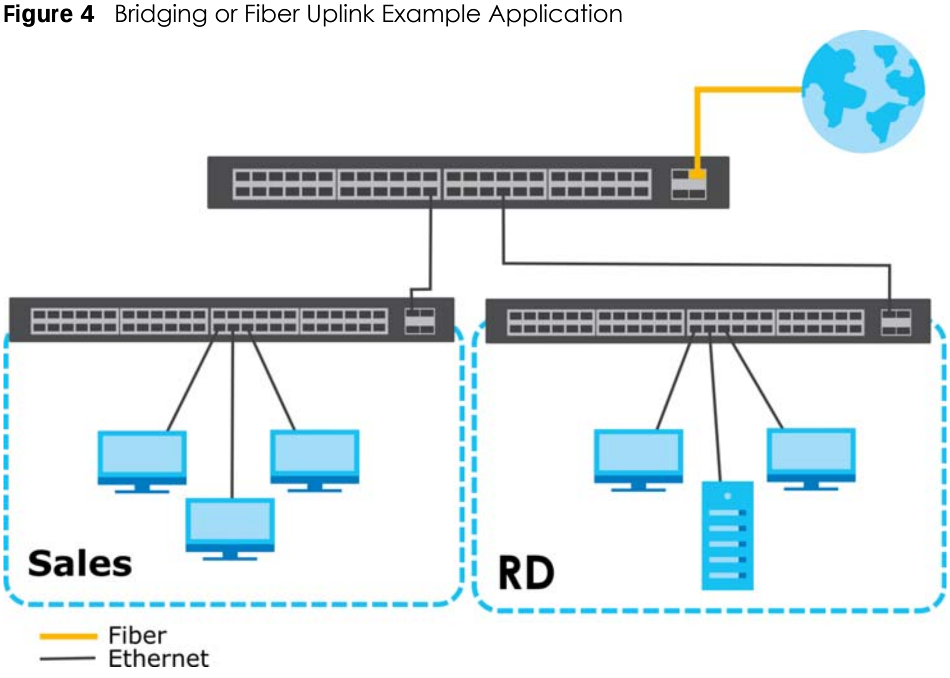
Figure 3 Backbone Application



1.2.3 Bridging or Fiber Uplink Example Application

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 a Gigabit Ethernet or SFP port on the Switch.

Figure 4 Bridging or Fiber Uplink Example Application



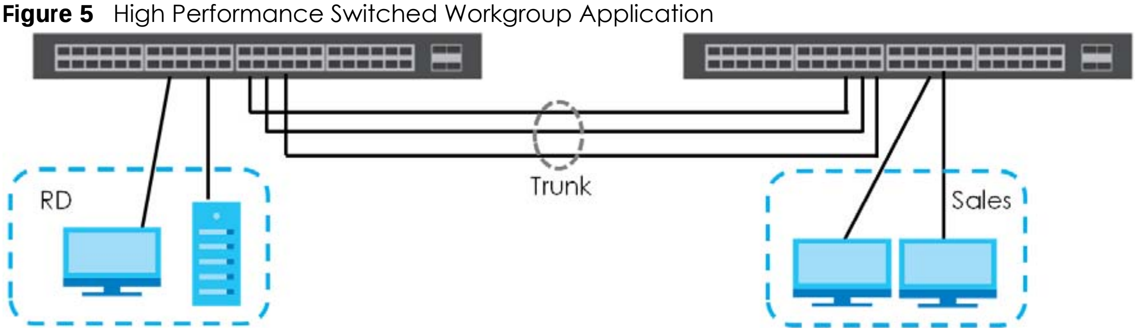
1.2.4 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use link aggregation (trunking) to connect these two networks.

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The Switch can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

This helps you switch to higher-speed LANs without the need for replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance.

Figure 5 High Performance Switched Workgroup Application



1.2.5 IEEE 802.1Q VLAN Application Examples

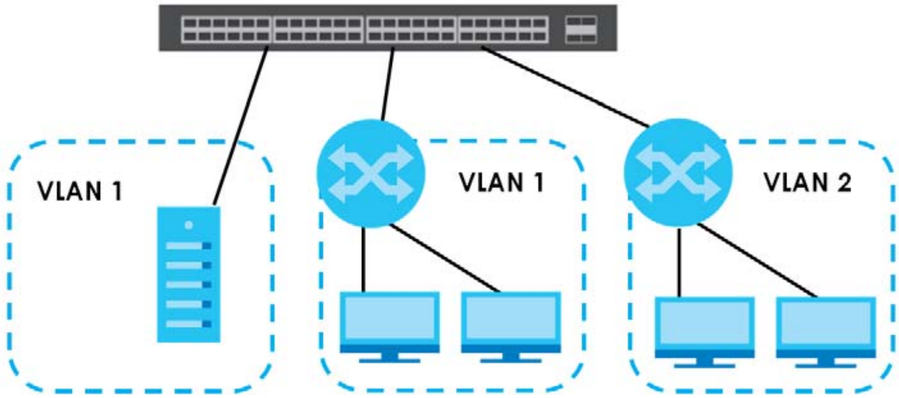
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same groups unless such traffic first goes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

1.2.5.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced 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 6 Shared Server Using VLAN Example



1.2.6 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, SSH, 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 C on page 533 and the CLI Reference Guide.

1.3 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- NCC (Zyxel Nebula Control Center). With the NCC, you can remotely manage and monitor the Switch through a cloud-based network management system. See Section 8.11 on page 131 or the NCC User's Guide for detailed information about how to access the NCC and manage your Switch via the NCC. See the NCC User's Guide for how to configure Nebula managed devices.
- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 50.
- Command Line Interface. Line commands offer an alternative to the Web Configurator and in some cases are necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See Section 46.9.1 on page 403.
- SNMP. The Switch can be monitored and/or managed by an SNMP manager. See Section 47.7.1 on page 416.

- Cluster Management. Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See Chapter 51 on page 437.
- ZON Utility. ZON Utility is a program designed to help you deploy and perform initial setup on a network more efficiently. See Section 4.3 on page 54.

1.4 Good Habits for Managing the Switch

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

- Change the password. Use a password that is 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.

CHAPTER 2
Hardware Installation and Connection

2.1 Installation Scenarios

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

The Switch can be:

- Placed on a desktop.
- Wall-mounted on a wall.
- Rack-mounted on a standard EIA rack.

See Table 1 on page 24 for the comparison table of the hardware installation methods for each model.

2.2 Safety Precautions

Please observe the following before using the Switch:

- It is recommended to ask an authorized technician to attach the Switch on a desk or to the rack or wall. Use the proper screws to prevent damage to the Switch. See the **Installation Requirements** sections in this chapter to know the types of screws and screw drivers for each mounting method.
- Make sure there is at least 2 cm of clearance on the top and bottom of the Switch, and at least 5 cm of clearance on all four sides of the Switch. This allows air circulation for cooling.
- Do NOT block the ventilation holes nor store cables or power cords on the Switch. Allow clearance for the ventilation holes to prevent your Switch from overheating. This is especially crucial when your Switch does not have fans. Overheating could affect the performance of your Switch, or even damage it.
- The surface of the Switch could be hot when it is functioning. Do NOT put your hands on it. You may get burned. This could happen especially when you are using a fanless Switch.
- The Switches with fans are not suitable for use in locations where children are likely to be present.

To start using the Switch, simply connect the power cables and turn it on.

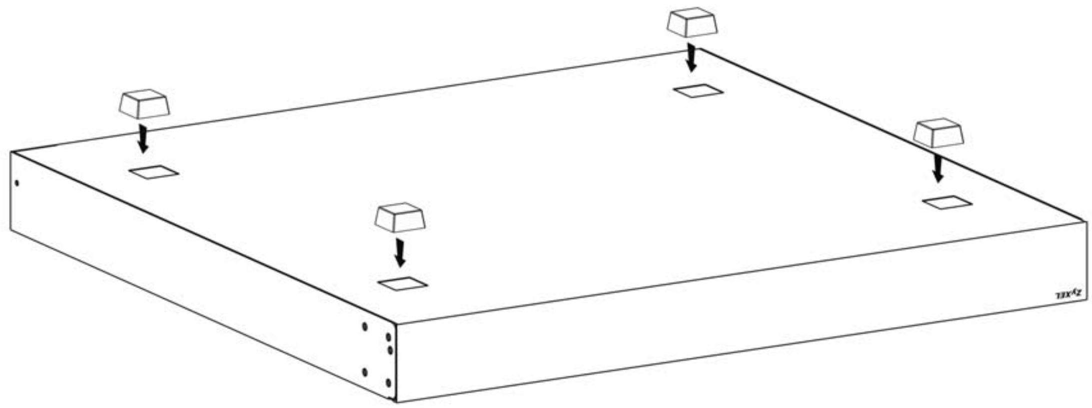
2.3 Desktop Installation Procedure

1 Make sure the Switch is clean and dry.

2 Remove the adhesive backing from the rubber feet.

3 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 7 Attaching Rubber Feet



4 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.

Cautions:

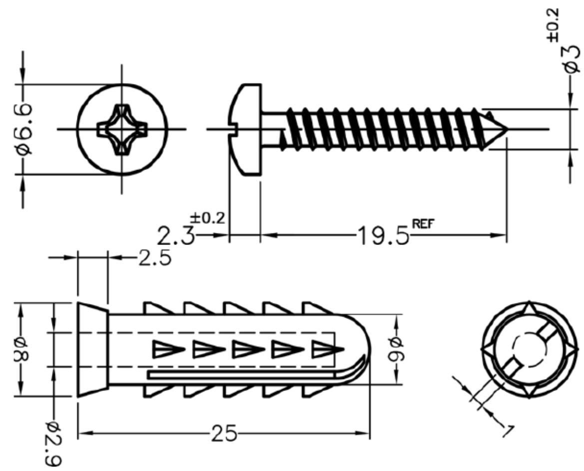
- Avoid stacking fanless Switches to prevent overheating.
- Ensure enough clearance around the Switch to allow air circulation for cooling.
- Do NOT remove the rubber feet as it provides space for air circulation.

2.4 Wall Mounting (GS2220-10 and GS2220-10HP Only)

The Switch can be mounted on a wall (see Table 1 on page 24). You may need screw anchors if mounting on a concrete or brick wall.

2.4.1 Installation Requirements

- Distance above the floor: At least 1.8 m (5.9 feet)
- Distance between holes: 78 mm (3.071 inches)
- Two M4 screws and a #2 Philips screwdriver
- Two screw anchors (optional)



1 Select a position free of obstructions on a wall strong enough to hold the weight of the Switch.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

WARNING! Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

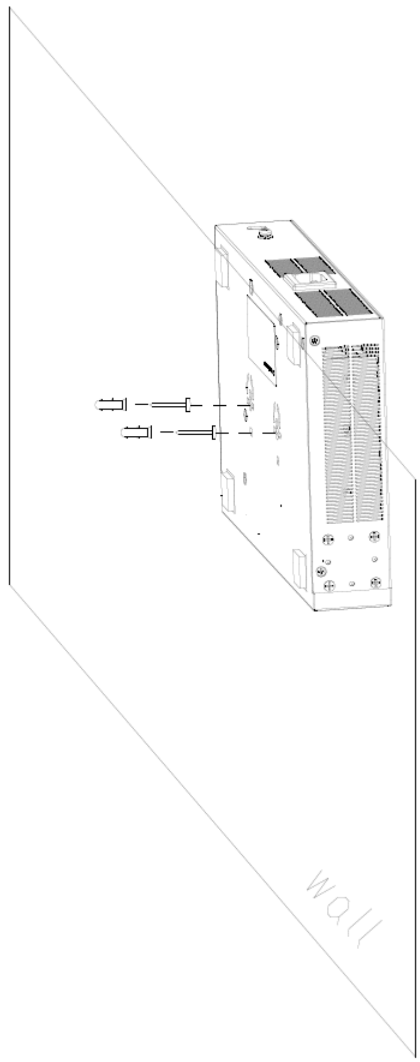
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do NOT insert the screws all the way in – leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do NOT insert the screws all the way in – leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the Switch with the connection cables.

5 Align the holes on the back of the Switch with the screws on the wall. Hang the Switch on the screws.

Note: Make sure there is enough clearance between the wall and the Switch to allow ventilation.



WARNING! The Switch should be wall-mounted horizontally, and make sure the front panel is facing down. The Switch's side panels with ventilation slots should not be facing up or down as this position is less safe.

2.5 Mounting the Switch on a Rack

The Switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment (see Table 1 on page 24). Follow the steps below to mount your Switch on a standard EIA rack using a rack-mounting kit.

Note: Make sure there is enough clearance between each equipment on the rack for air circulation.

2.5.1 Installation Requirements

- Two mounting brackets.

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

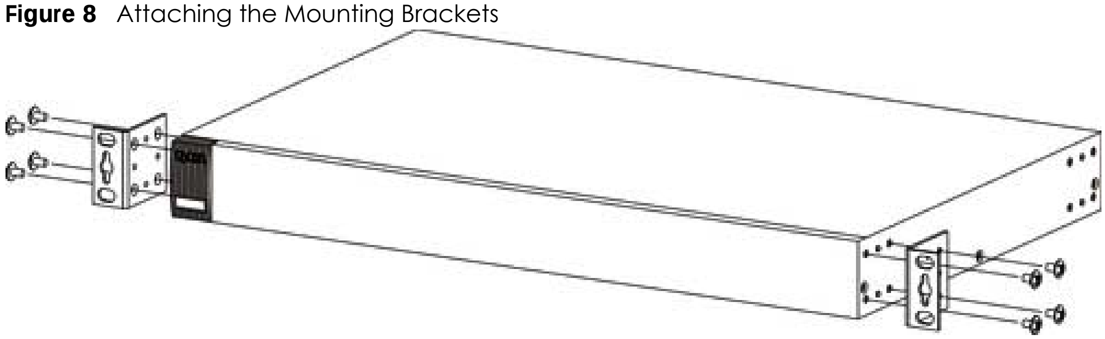
2.5.2 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains. The maximum weight a bracket can hold is 21.5 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.

2.5.3 Attaching the Mounting Brackets to the Switch

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

Figure 8 Attaching the Mounting Brackets



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

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

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

2.5.4 Mounting the Switch on a Rack

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

Figure 9 Mounting the Switch on a Rack

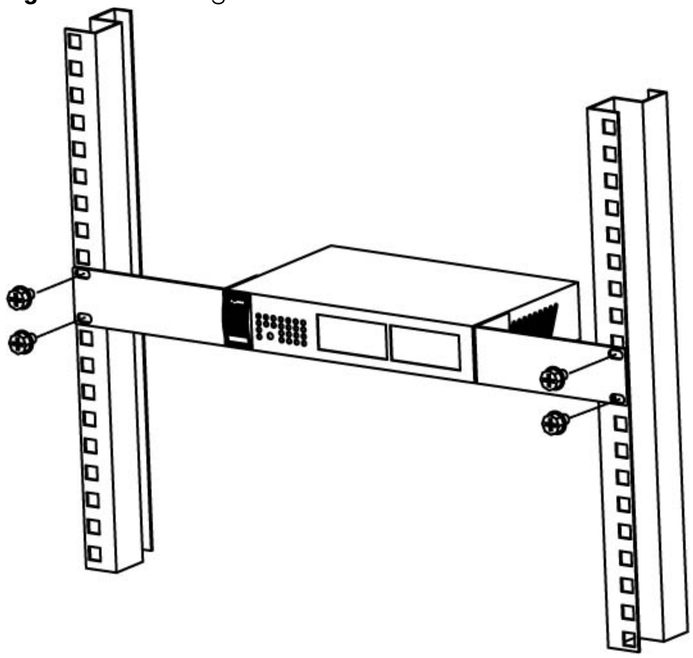
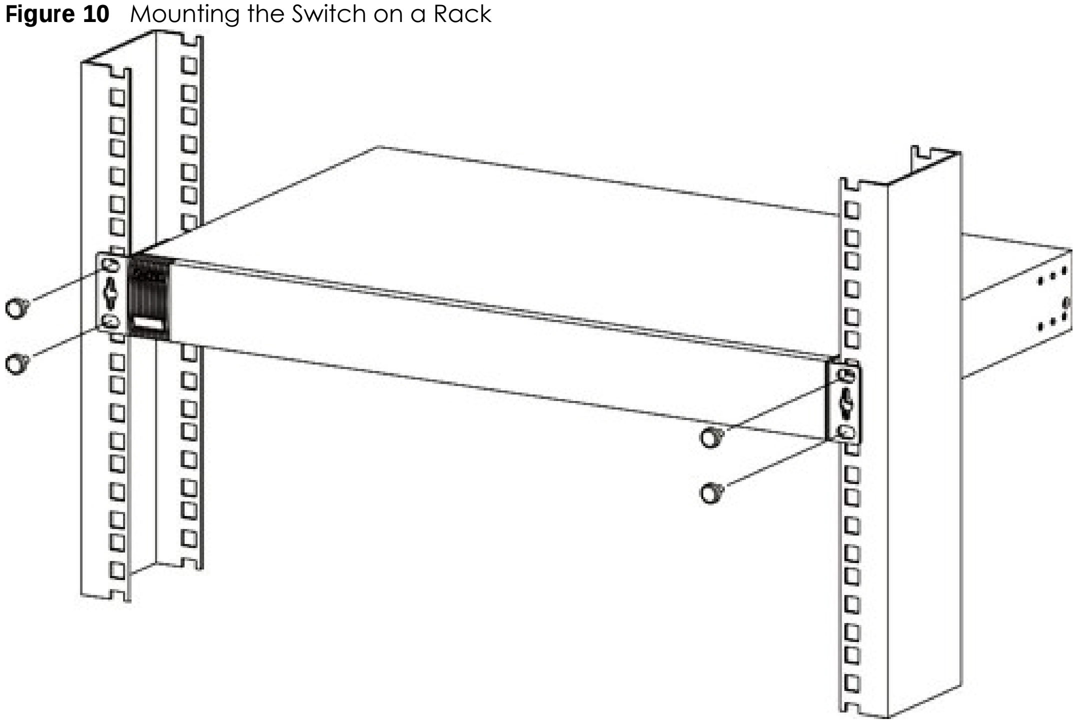


Figure 10 Mounting the Switch on a Rack



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

Note: Make sure you tighten all the four screws to prevent the Switch from getting slanted.

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

CHAPTER 3
Hardware Panels

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 following figures show the front panels of the Switch.

Figure 11 Front Panel: GS2220-10

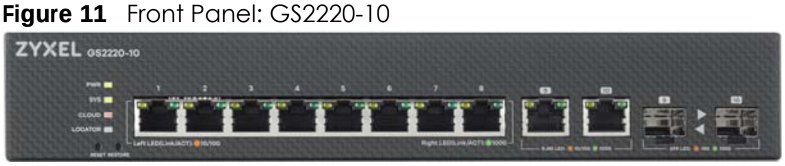


Figure 12 Front Panel: GS2220-10HP

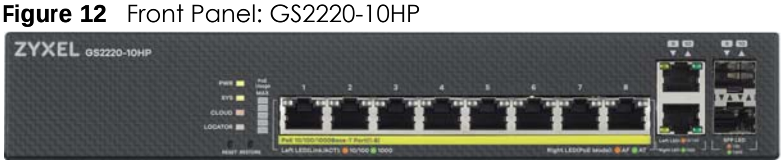


Figure 13 Front Panel: GS2220-28

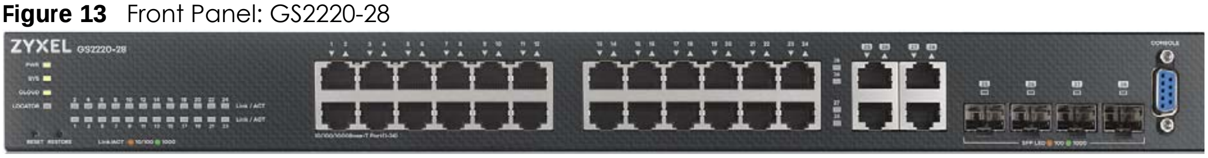


Figure 14 Front Panel: GS2220-28HP

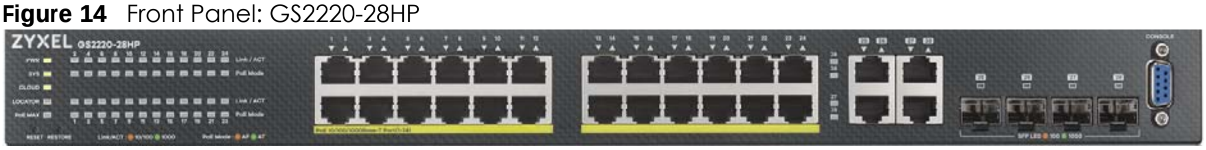


Figure 15 Front Panel: GS2220-50

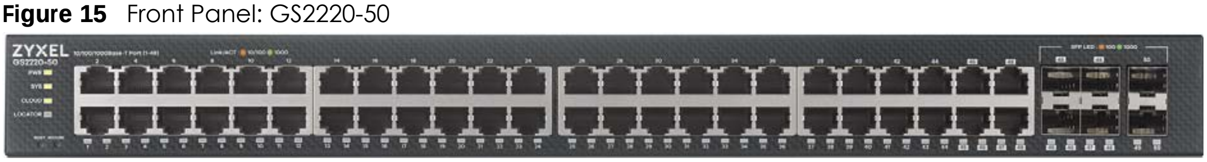
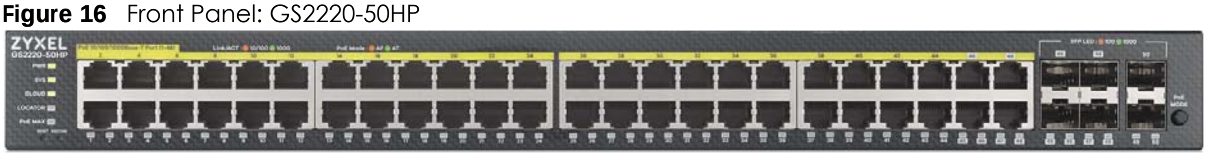


Figure 16 Front Panel: GS2220-50HP



The following table describes the ports.

Table 3 Panel Connections

CONNECTOR	DESCRIPTION
8/24/48 1000Base-T RJ-45 Ethernet Ports	These are 10/100/1000Base-T auto-negotiating and auto-crossover Ethernet ports. Connect these ports to a computer, a hub, a router, or an Ethernet switch.
2 SFP Slots (only available for GS2220-50/50HP)	Use SFP transceivers in these ports for high-bandwidth backbone connections.
2/4 GbE Combo Ports (Dual Personality Interfaces)	Each interface has one 10/100/1000Base-T copper RJ-45 port and one SFP slot, with one port active at a time.
	• 10/100/1000Base-T Ports: Connect these ports to a computer, an Ethernet switch or router.
	• SFP Slots: Use Small Form-Factor Pluggable (SFP) transceivers in these ports for fiber connections to an Ethernet switch or router.
Reset	Press the **RESET** button to reboot the Switch without turning the power off. See Section 3.3 on page 47 for more information about the LED behavior.
Restore	Press the **RESTORE** button for 3 to 7 seconds to have the Switch automatically reboot and restore the last-saved custom default file. See Section 3.3 on page 47 for more information about the LED behavior. Press the **RESTORE** button for more than 7 seconds to have the Switch automatically reboot and restore the factory default file. See Section 3.3 on page 47 for more information about the LED behavior.
PoE Mode (only available for GS2220-50HP)	Push or release this button to change how the **Link/ACT** LED works. • Each Ethernet port's LED is changed to act as a **PoE Mode** LED by pushing the **PoE MODE** button on the front panel. • Each Ethernet port's LED is changed back to act as a **Link/ACT** LED by releasing the PoE **MODE button** on the front panel. View the LEDs to ensure proper functioning of the Switch and as an aid in troubleshooting (see Section 3.3 on page 47).
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 Gigabit Ethernet Ports

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

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

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

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

Note: The dual personality ports change to fiber mode directly when inserting the fiber module.

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

3.1.1.1 Default Ethernet Negotiation Settings

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

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

3.1.1.2 Auto-crossover

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

3.1.2 PoE (GS2220-10HP, GS2220-28HP and GS2220-50HP)

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

3.1.3 SFP Slots

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

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

- Type: SFP connection interface
- Connection speed: 100/1000 Mbps

WARNING! To avoid possible eye injury, do not look into an operating fiber module's connectors.
HANDLING! All transceivers are static sensitive. To prevent damage from electrostatic discharge (ESD), it is recommended you attach an ESD preventive wrist strap to your wrist and to a bare metal surface when

you install or remove a transceiver.
STORAGE! All modules are dust sensitive. When not in use, always keep the dust plug on. Avoid getting dust and other contaminant into the optical bores, as the optics do not work correctly when obstructed with dust.

3.1.3.1 Transceiver Installation

Use the following steps to install a transceiver.

1. Attach an ESD preventive wrist strap to your wrist and to a bare metal surface.
2. Align the transceiver in front of the slot opening.
3. Make sure the latch is in the lock position (latch styles vary), then insert the transceiver into the slot with the exposed section of PCB board facing down.
4. Press the transceiver firmly until it clicks into place.
5. The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
6. Remove the dust plugs from the transceiver and cables (dust plug styles vary).
7. Identify the signal transmission direction of the fiber cables and the transceiver. Insert the fiber cable into the transceiver.

Figure 17 Latch in the Lock Position

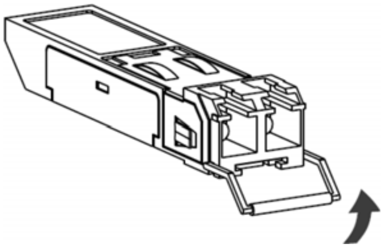


Figure 18 Transceiver Installation Example

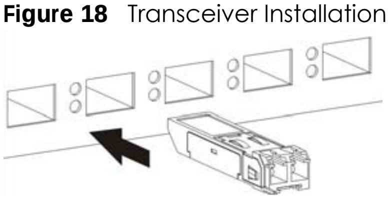
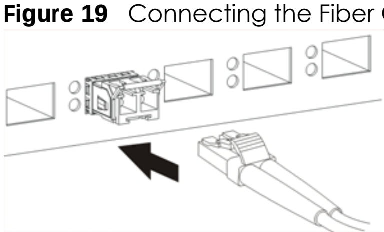


Figure 19 Connecting the Fiber Cables



3.1.3.2 Transceiver Removal

Use the following steps to remove an SFP transceiver.

1 Attach an ESD preventive wrist strap to your wrist and to a bare metal surface on the chassis.

2 Remove the fiber cables from the transceiver.

3 Pull out the latch and down to unlock the transceiver (latch styles vary).

Note: Make sure the transceiver's latch is pushed all the way down, so the transceiver can be pulled out successfully.

4 Pull the latch, or use your thumb and index finger to grasp the tabs on both sides of the transceiver, and carefully slide it out of the slot.

Note: Do NOT pull the transceiver out by force. You could damage it. If the transceiver will not slide out, grasp the tabs on both sides of the transceiver with a slight up or down motion and carefully slide it out of the slot. If unsuccessful, contact Zyxel Support to prevent damage to your Switch and transceiver.

5 Insert the dust plug into the ports on the transceiver and the cables.

Figure 20 Removing the Fiber Cables

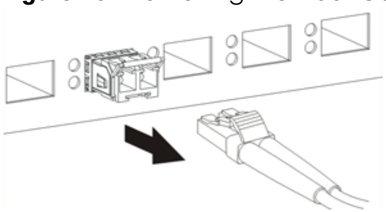


Figure 21 Opening the Transceiver's Latch Example

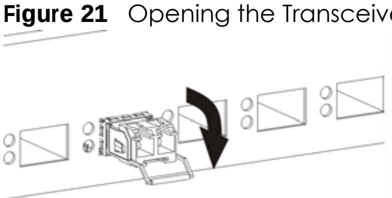
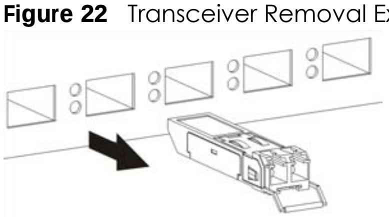


Figure 22 Transceiver Removal Example



3.1.4 Dual Personality Interfaces

A combo port is for uplink connections. It consists of a Gigabit Ethernet port for Ethernet connection, and a SFP transceiver slot for fiber connection. The fiber connection takes priority if the corresponding Gigabit port is also connected.

- 100 Mbps/1 Gbps – Connect these ports to high-bandwidth backbone network Ethernet switches.
- Transceiver Slots – Use SFP transceivers in these slots for connections to backbone Ethernet switches.

Figure 23 Combo Port Example: Gigabit Port and SFP Transceiver Slot

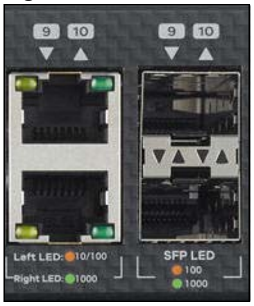


Figure 24

3.1.5 Console Port

This console port is for troubleshooting only. With instructions from customer support, 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. You can use a computer with terminal emulation software configured to the following parameters:

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

3.2 Rear Panel

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

Figure 25 Rear Panel: GS2220-10

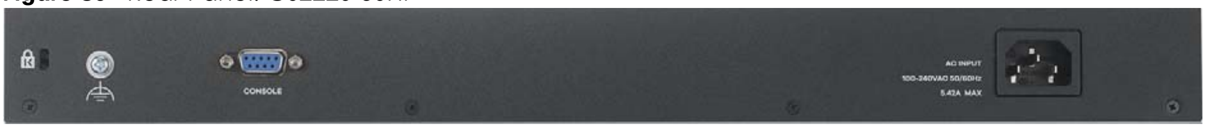
Figure 26 Rear Panel: GS2220-10HP

Figure 27 Rear Panel: GS2220-28

Figure 28 Rear Panel: GS2220-28HP

Figure 29 Rear Panel: GS2220-50

Figure 30 Rear Panel: GS2220-50HP



3.2.1 Grounding

Grounding is a safety measure to direct excess electric charge to the ground. It prevents damage to the Switch, and protects you from electrocution. Use the grounding screw on the rear panel and the ground wire of the AC power supply to ground the Switch.

The grounding terminal and AC power ground where you install the Switch must follow your country's regulations. Qualified service personnel must ensure the building's protective earthing terminals are valid terminals.

Installation of Ethernet cables must be separate from AC power lines. To avoid electric surge and electromagnetic interference, use a different electrical conduit or raceway (tube/trough or enclosed conduit for protecting electric wiring) that is 15 cm apart, or as specified by your country's electrical regulations.

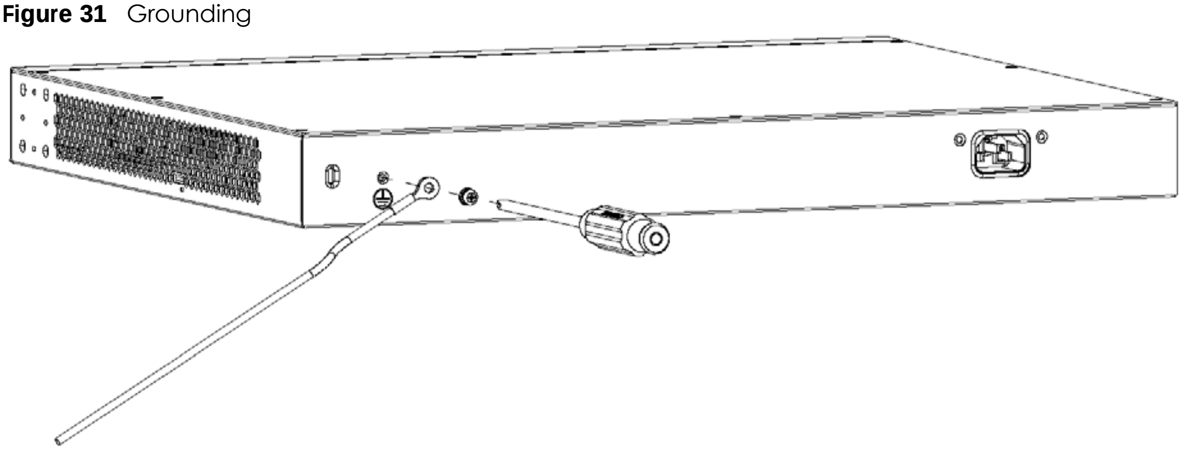
Any device that is located outdoors and connected to this product must be properly grounded and surge protected. To the extent permissible by your country's applicable law, failure to follow these guidelines could result in damage to your Switch which may not be covered by its warranty.

Note: The specification for surge or ESD protection assumes that the Switch is properly grounded.

1 Remove the M4 ground screw from the Switch's rear panel.

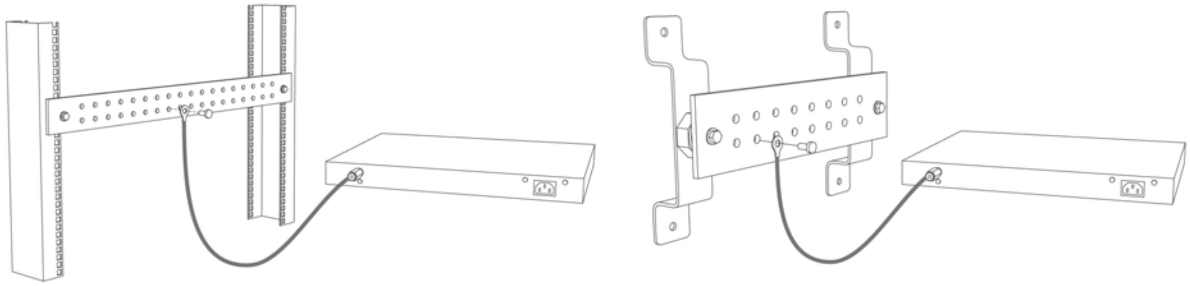
2 Secure a green or yellow ground cable (16 AWG or smaller) to the Switch's rear panel using the M4 ground screw.

Figure 31 Grounding



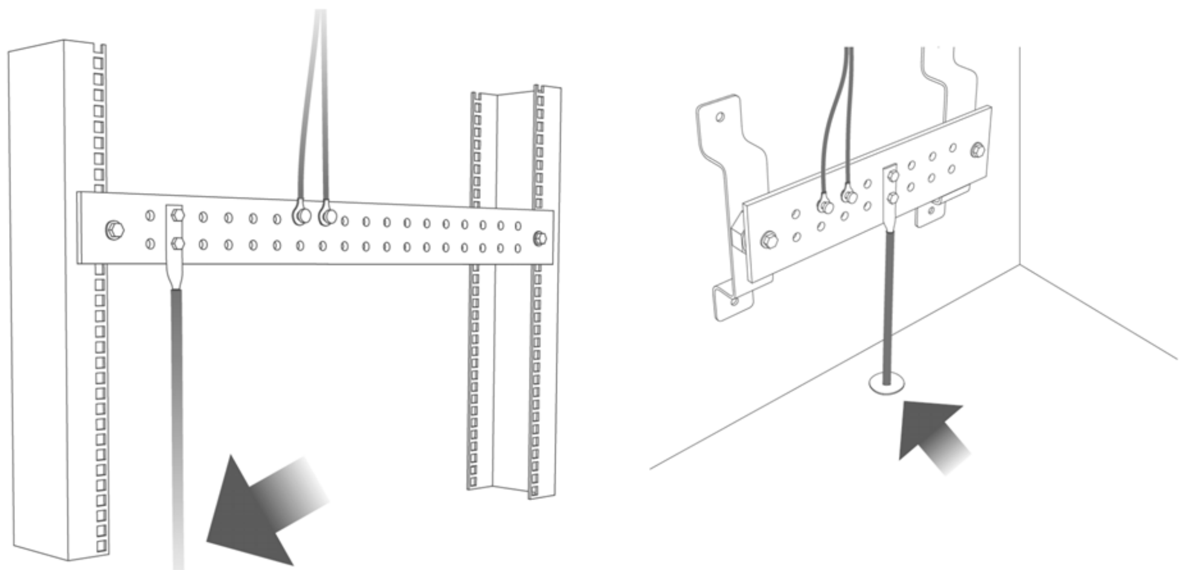
3 Attach the other end of the ground cable to a grounding bar located on the rack where you install the Switch or to an on-site grounding terminal.

Figure 32 Attach Ground Cable to Grounding Bar or On-site Grounding Terminal



4 The grounding terminal of the server rack or on-site grounding terminal must also be grounded and connected to the building's main grounding electrode. Make sure the grounding terminal is connected to the buildings grounding electrode and has an earth resistance of less than 10 ohms, or according to your country's electrical regulations.

Figure 33 Connecting to the Building's Main Grounding Electrode



If you are uncertain that suitable grounding is available, contact the appropriate electrical inspection authority or an electrician.

This device must be grounded. Do this before you make other connections.

3.2.2 AC Power Connection

Note: Make sure you are using the correct power source as shown on the panel and that no objects obstruct the airflow of the fans (located on the side of the unit).

To connect power to the Switch, insert the female end of the power cord to the AC power receptacle on the rear panel. Connect the other end of the supplied power cord to a power outlet.

3.3 LEDs

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

Table 4 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Switch is receiving power from the power module in the power slot.
		Blinking	The Switch is returning to the last-saved custom default configuration settings.
	Amber	On	The Switch is returning to its factory default configuration settings.
		Off	The Switch is not receiving power from the power module in the power slot.
SYS	Green	On	The Switch is on and functioning properly.
		Blinking	The Switch is rebooting and performing self-diagnostic tests.
	Red	On	The Switch is functioning abnormally.
		Off	The power is off or the Switch is not ready or malfunctioning.
CLOUD	Green	On	The Switch has successfully connected to the NCC (Nebula Control Center).
		Blinking	The Switch cannot connect to the NCC because it is not registered.
	Amber	On	The Switch is registered at NCC but cannot connect to the NCC. Please check the Internet connection of the Switch.
		Blinking	The Switch is not registered at NCC and cannot connect to the NCC. Please check the Internet connection of the Switch and register the Switch at NCC.
		Off	The Switch is operating in standalone mode. Nebula Control Center Discovery is disabled in **Basic** > **Cloud Management** > **Nebula Control Center Discovery** in the Switch's Web Configurator.
LOCATOR	Blue	On	The Switch is uploading firmware. While the Switch is doing this, do NOT turn off the power.
		Blinking	Shows the actual location of the Switch between several devices in a rack. The default timer is 30 minutes when you are configuring the Switch.
		Off	The locator is not functioning or malfunctioning.
PoE Usage MAX (GS2220-10HP) Bar1 is the bar at the bottom; bar 5 is the bar at the top.	Green (Bar1 – Bar3)	On	Each bar represents 20 percent of PoE Power consumption. **Bar 1**: PoE power usage is below 20 percent of the power supplied budget. **Bar 2**: PoE power usage is below 40 percent of the power supplied budget, but over 20 percent of the power supplied budget. **Bar 3**: PoE power usage is below 60 percent of the power supplied budget, but over 40 percent of the power supplied budget.
	Yellow (Bar4)	On	PoE power usage is below 80 percent of the power supplied budget, but over 60 percent of the power supplied budget.
	Red (Bar5)	On	PoE power usage is more than 80 percent of the power supplied budget.
		Blinking	Less than 5 percent of the power supplied budget remains. 5 percent is the default value.
		Off	PoE power usage is 0 percent of the power supplied budget.
PoE MAX (GS2220-28HP and GS2220-50HP)	Amber	On	Less than five percent of the power supplied budget remains. Five percent is the default value.
		Off	The Switch has a sufficient power supplied budget.
Ethernet Ports and PoE			

Table 4 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
LNK/ACT	Green	Blinking	The Switch is transmitting/receiving to/from a 1000 Mbps Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The Switch is transmitting/receiving to/from a 10 Mbps or a 100 Mbps Ethernet network.
		On	The link to a 10 Mbps or a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
PoE Mode (GS2220-10HP, GS2220-28HP and GS2220-50HP)	Green	On	Power supplied to all PoE Ethernet ports meets the IEEE 802.3at standard.
	Amber	On	Power supplied to all PoE Ethernet ports meets the IEEE 802.3af standard.
		Off	There is no power supplied.
SFP Slots			
LINK/ACT	Green	On	The uplink port is linking at 1000 Mbps.
		Blinking	The Switch is transmitting or receiving data at 1000 Mbps.
	Amber	On	The uplink port is linking at 100 Mbps.
		Blinking	The Switch is transmitting or receiving data at 100 Mbps.
		Off	There is no link or port, or the uplink port is shut down.

PART II
Technical Reference

CHAPTER 4
Web Configurator

4.1 Overview

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

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such Microsoft Edge, Internet Explorer 11, Mozilla Firefox, or Google Chrome. 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.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

1 Start your web browser.

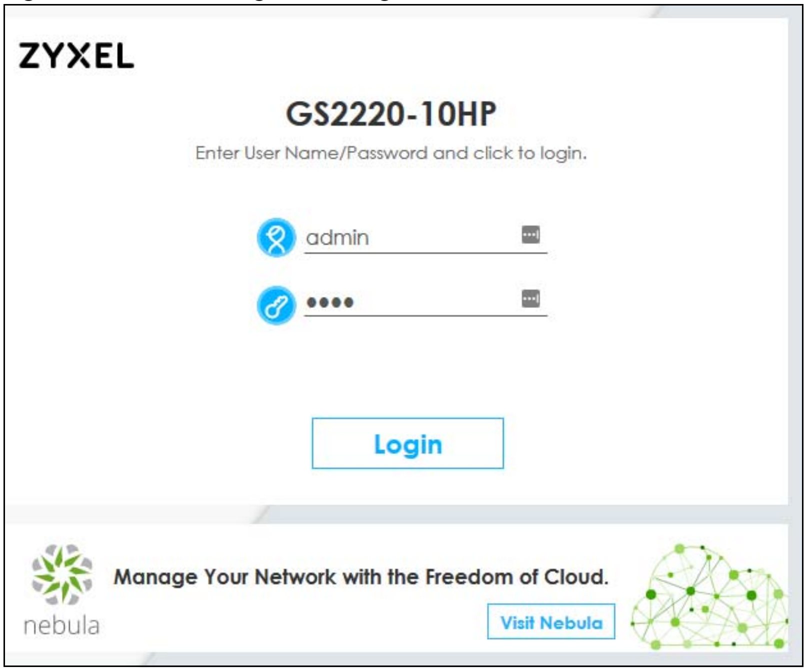
2 The Switch is a DHCP client by default. Type "http://DHCP-assigned IP" in the **Location** or **Address** field. Press [ENTER].

   If the Switch is not connected to a DHCP server, type "http://" and the static IP address of the Switch (for example, the default management IP address is 192.168.1.1 through an in-band port) in the **Location** or **Address** field. Press [ENTER]. Your computer must be in the same subnet in order to access this website address.

   Also, you can use the ZON Utility to check your Switch's IP address. See Section 4.3 on page 54 for more information on the ZON utility.

3 The following screen appears.

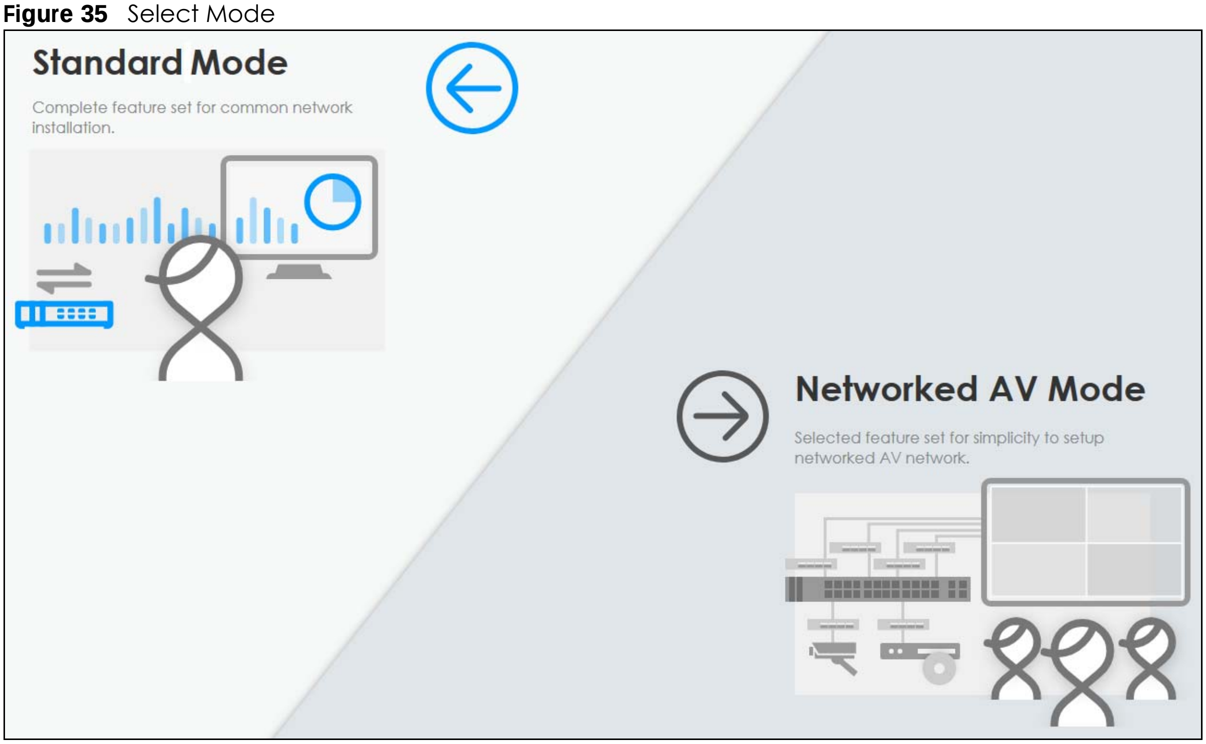
Figure 34 Web Configurator: Login



4 Click **Login** to log into the Web Configurator to manage the Switch directly. The default user name is **admin** and associated default password is **1234**.

5 The following screen appears.

Figure 35 Select Mode



6 Select the Web Configurator in **Standard Mode** that has a complete set of configuration for network installation. Or select the Web Configurator in **Networked AV Mode** that has a set of menus specifically designed to simplify configuration and management of the Switch for AVoIP (Audio-Video over Internet Protocol) application (Chapter 58 on page 461).

7 If you select **Standard Mode**, go directly to step 9.

8 The **Setup Wizard** screen will appear after selecting the **Networked AV Mode**. You can use the **Setup Wizard** screen to configure the Switch's Networked AV mode's basic or advanced settings.

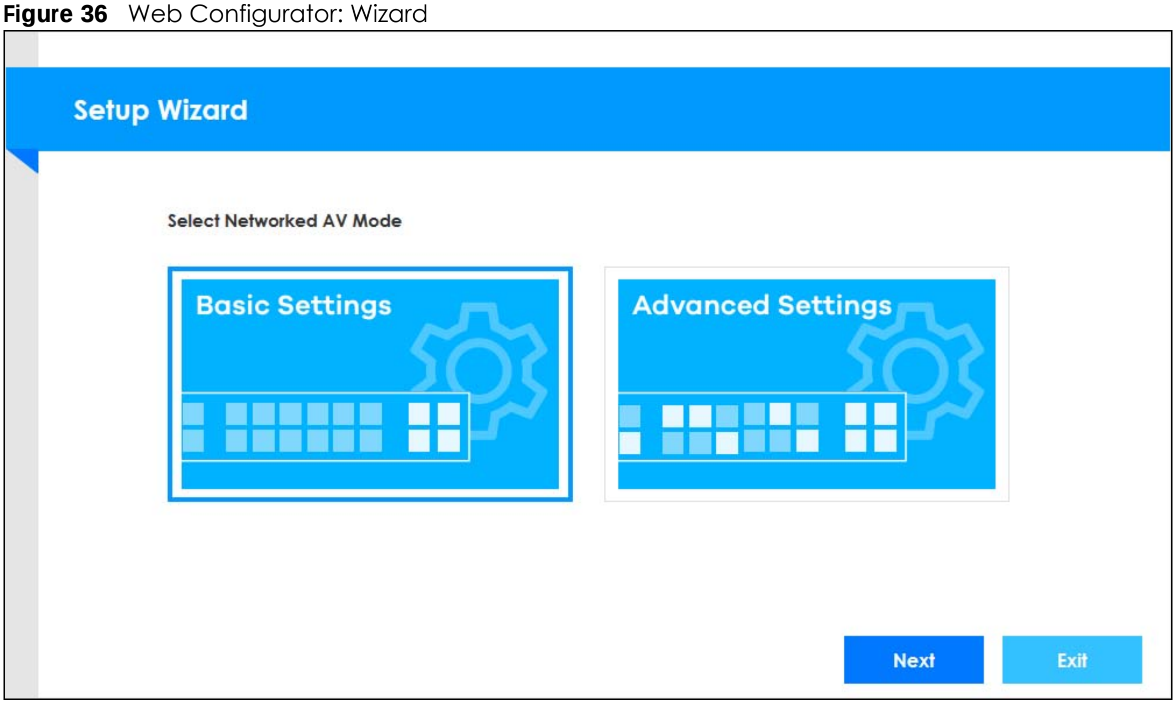
- Use the **Basic Settings** to configure networked AV operation on management VLAN. Such as the Switches' IP address, DNS server, system password, SNMP community, accept or skip the default Networked AV mode settings, and view a summary of the basic settings.
- Use the **Advanced Settings** for networks that wants to separate networked AV VLAN from management VLAN, specify which ports connect to AVoIP application, and for setting link aggregation across switches.

See Section 4.4 on page 58 for more information on the **Setup Wizard** screen.

Once you click the **Finish** button, the settings configured in the **Setup Wizard** screen will overwrite the existing settings.

Otherwise, click the **Exit** button. If you want to open the **Setup Wizard** screen later, click the **Wizard** icon in the upper right hand corner of the Web Configurator in Networked AV mode.

Figure 36 Web Configurator: Wizard



9 If you did not change the default administrator password and/or SNMP community values, a warning screen displays each time you log into the Web Configurator and select **Standard Mode**. Click **Password / SNMP** to open a screen where you can change the administrator password and SNMP community string simultaneously. Otherwise, click **Ignore** to close it.
If you log into the Web Configurator and select **Networked AV Mode**, open the screen in the **Wizard** > **Step 2 Password** to change the administrator password and SNMP community string. Click **Finish** on the last step of the **Wizard** to save your settings.

Password/SNMP Setting

Figure 37 Web Configurator: Warning

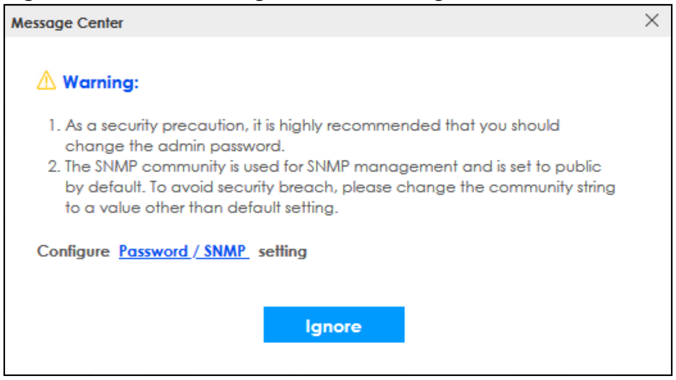
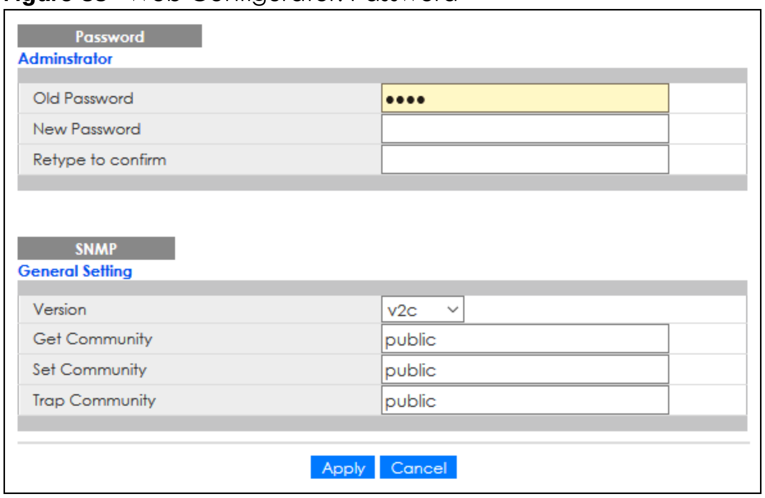


Figure 38 Web Configurator: Password



Change the default administrator and/or SNMP passwords, and then click **Apply** to save your changes.

Table 5 Web Configurator: Password/SNMP

LABEL	DESCRIPTION
Administrator This is the default administrator account with the "admin" user name. You cannot change the default administrator user name.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation.
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.

Table 5 Web Configurator: Password/SNMP (continued)

LABEL	DESCRIPTION
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.
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.

4.3 Zyxel One Network (ZON) Utility

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 computer (Windows operating system).

4.3.1 Requirements

Before installing the ZON Utility on your computer, please make sure it meets the requirements listed below.

Operating System

At the time of writing, the ZON Utility is compatible with:

- Windows 7 (both 32-bit / 64-bit versions)
- Windows 8 (both 32-bit / 64-bit versions)
- Windows 8.1 (both 32-bit / 64-bit versions)
- Window 10 (both 32-bit / 64-bit versions)

Note: To check for your Windows operating system version, right-click on **My Computer** > **Properties**. You should see this information in the **General** tab.

Hardware

Here are the minimum hardware requirements to use the ZON Utility on your computer.

- Core i3 processor

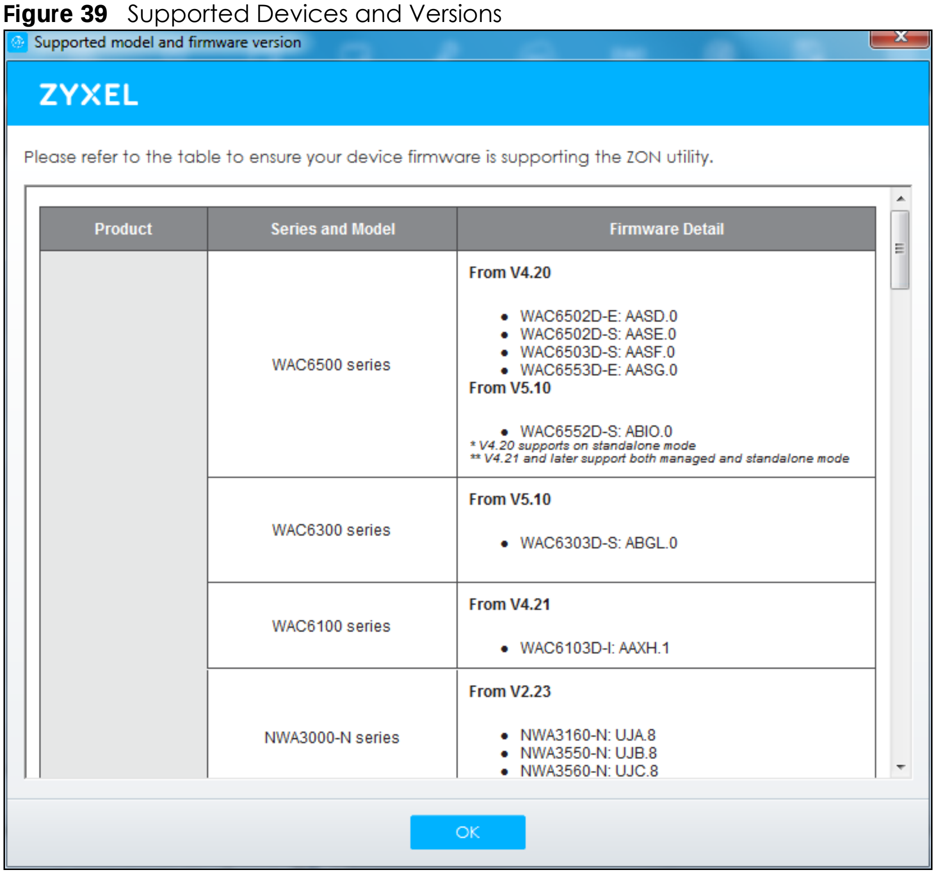
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280 by 800)

4.3.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

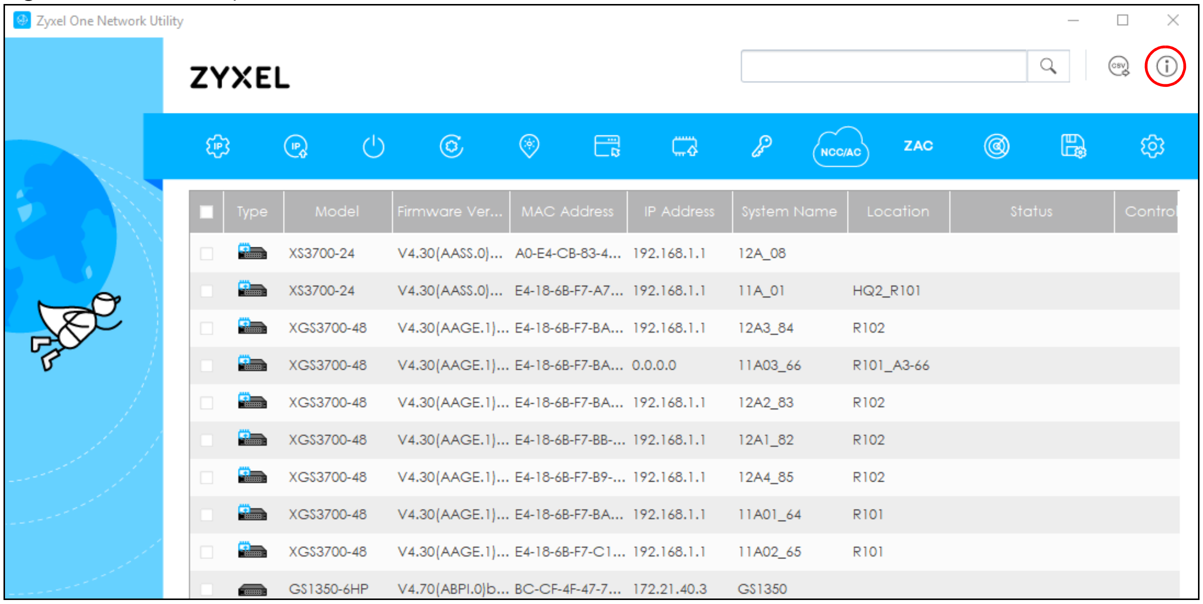
2 The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 39 Supported Devices and Versions



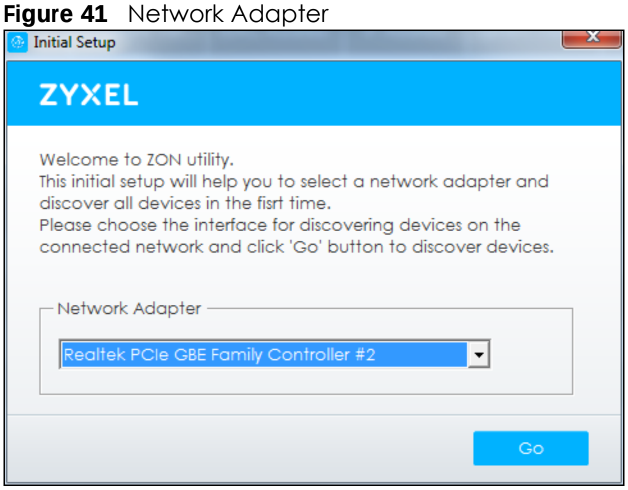
If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for ZON Utility support. The release notes are in the firmware zip file on the Zyxel web site.

Figure 40 ZON Utility Screen



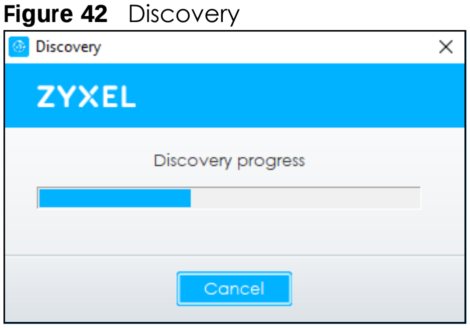
3 Select a network adapter to which your supported devices are connected.

Figure 41 Network Adapter



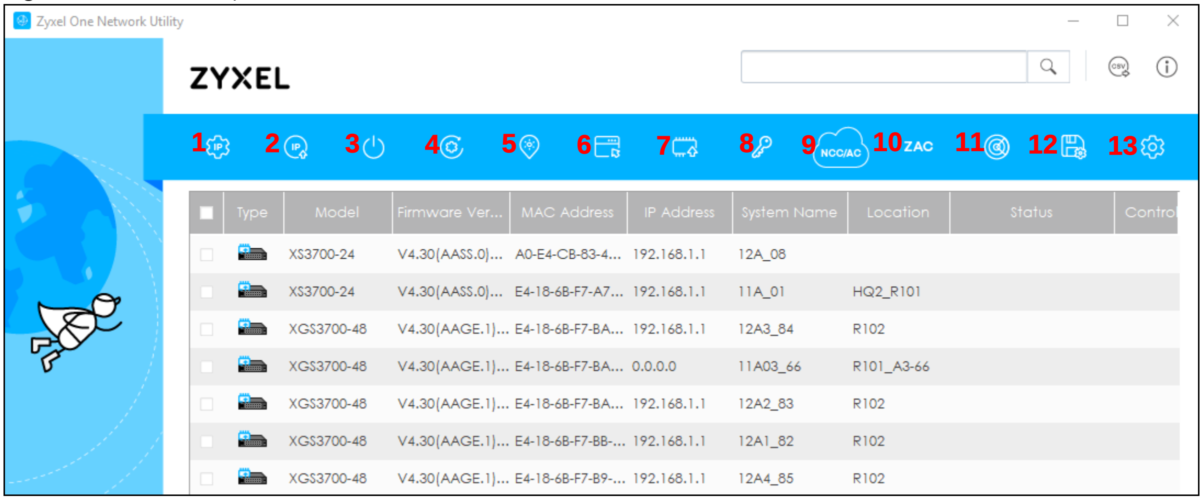
4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 42 Discovery



5 The ZON Utility screen shows the devices discovered.

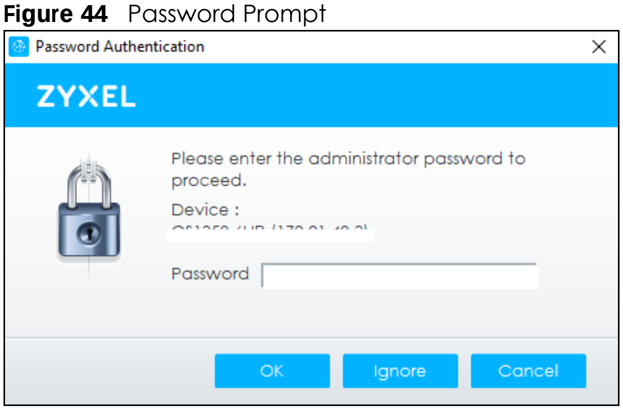
Figure 43 ZON Utility Screen



6 Select a device and then use the icons to perform actions. Some functions may not be available for your devices.

Note: You must know the selected device admin password before taking actions on the device using the ZON Utility icons.

Figure 44 Password Prompt



The following table describes the icons numbered from left to right in the ZON Utility screen.

Table 6 ZON Utility Icons

ICON	DESCRIPTION
1 IP Configuration	Change the selected device's IP address.
2 Renew IP Address	Update a DHCP-assigned dynamic IP address.
3 Reboot Device	Use this icon to restart the selected devices. This may be useful when troubleshooting or upgrading new firmware.
4 Reset Configuration to Default	Use this icon to reload the factory-default configuration file. This means that you will lose all previous configurations.
5 Locator LED	Use this icon to locate the selected device by causing its **Locator** LED to blink.
6 Web GUI	Use this to access the selected device Web Configurator from your browser. You will need a user name and password to log in.
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected devices of the same model. Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance.

Table 6 ZON Utility Icons

ICON	DESCRIPTION
8 Change Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.
9 Configure NCC Discovery	You must have Internet access to use this feature. Use this icon to enable or disable the Nebula Control Center (NCC) discovery feature on the selected device. If it is enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it will go into the Nebula cloud management mode.
10 ZAC	Use this icon to run the Zyxel AP Configurator of the selected AP.
11 Clear and Rescan	Use this icon to clear the list and discover all devices on the connected network again.
12 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device.
13 Settings	Use this icon to select a network adapter for the computer on which the ZON utility is installed, and the utility language.

The following table describes the fields in the ZON Utility main screen.

Table 7 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON Utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the Switch does not support **IP Configuration**, **Renew IP address** and **Flash Locator LED**, this field displays “Update failed”, “Not support Renew IP address” and “Not support Flash Locator LED” respectively.
Controller Discovery	This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature. If it is enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it will go into the Nebula cloud management mode.
Serial Number	Enter the admin password of the discovered device to display its serial number.
Hardware Version	This field displays the hardware version of the discovered device.

4.4 Wizard

The **Setup Wizard** contains the following parts:

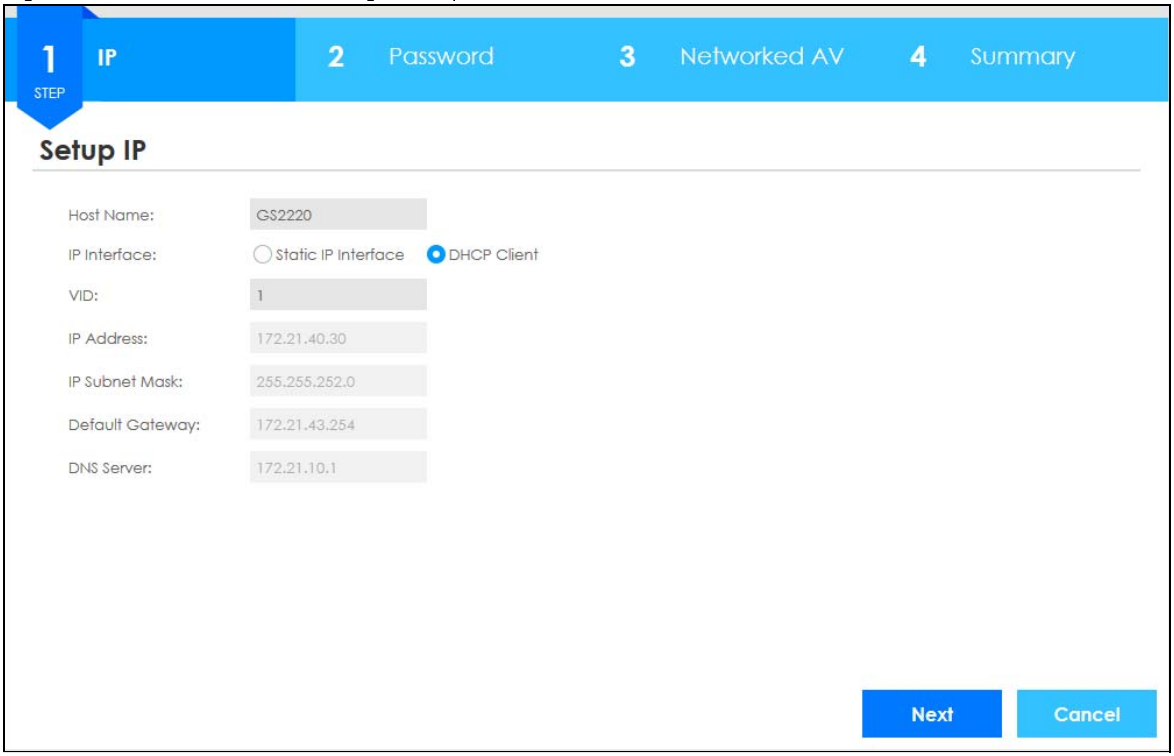
- Use the **Basic Settings** when networked AV service runs on management VLAN, using the combo/ fiber port for inter-switch connection.
- Use the **Advanced Settings** when you need to specify the VLAN for networked AV service and configure the port’s role manually.

4.4.1 Basic Settings

In **Basic Settings**, you can set up IP or DNS, set up your password, SNMP community, accept or skip the default Networked AV mode settings, and view finished results.

In order to set up your IP or DNS, please do the following. Click **Wizard** > **Basic Settings** > **Step 1 IP** to access this screen.

Figure 45 Wizard > Basic Settings > Step 1 IP



Each field is described in the following table.

Table 8 Wizard > Basic Settings > Step 1 IP

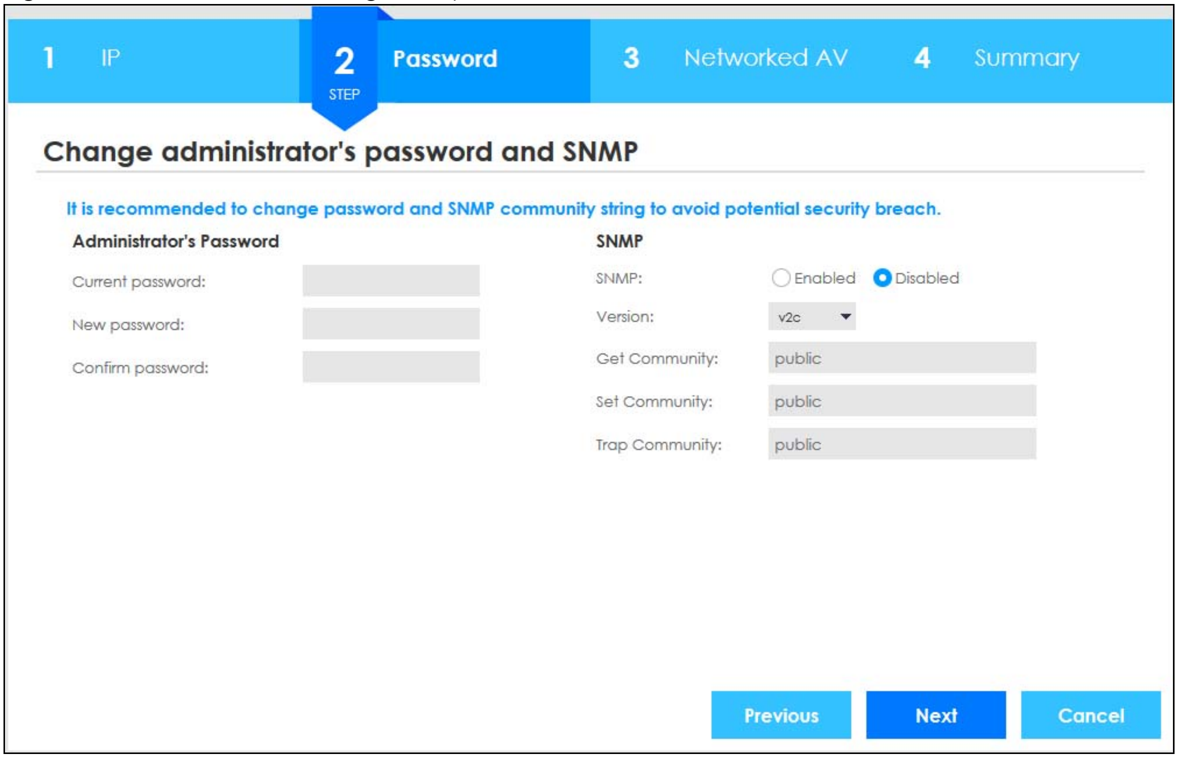
LABEL	DESCRIPTION
Host Name	This field displays a host name.
IP Interface	Select **DHCP Client** if the Switch is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Switch in order to access the Switch's Web Configurator again. Select **Static IP Interface** when the Switch is NOT connected to a router or you want to assign it a fixed IP address.
VID	This field displays the VLAN ID.
IP Address	The Switch needs an IP address for it to be managed over the network.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.

Table 8 Wizard > Basic Settings > Step 1 IP

LABEL	DESCRIPTION
Next	Click **Next** to show the next screen.
Cancel	Click **Cancel** to exit this screen without saving.

After clicking **Next,** the **Password** screen appears.

Figure 46 Wizard > Basic Settings > Step 2 Password



Each field is described in the following table.

Table 9 Wizard > Basic Settings > Step 2 Password

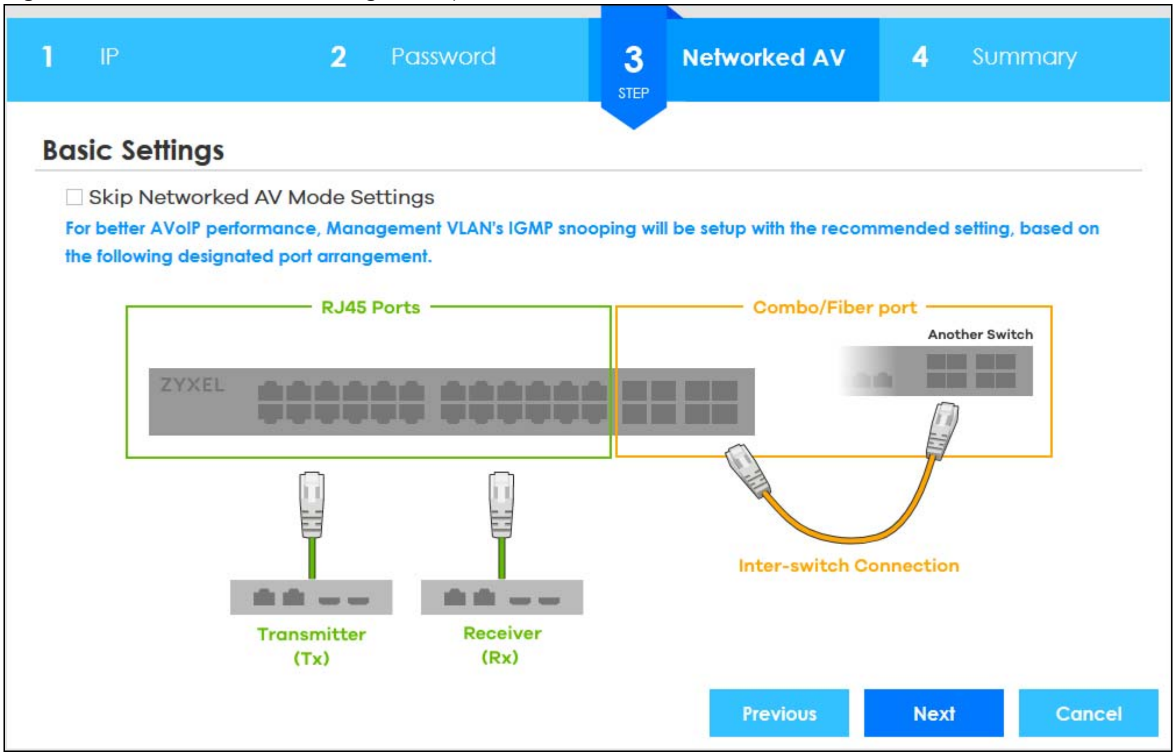
LABEL	DESCRIPTION
Administrator's Password	
Current password	Type the existing system password (1234 is the default password when shipped).
New password	Enter your new system password.
Confirm password	Retype your new system password for confirmation.
SNMP	
SNMP	Select **Enabled** to let the Switch act as an SNMP agent, which allows a manager station to manage and monitor the Switch through the network. Select **Disabled** to turn this feature off.
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.

Table 9 Wizard > Basic Settings > Step 2 Password (continued)

LABEL	DESCRIPTION
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNextrequests 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.
Previous	Click **Previous** to show the previous screen.
Next	Click **Next** to show the next screen.
Cancel	Click **Cancel** to exit this screen without saving.

After clicking **Next**, the **Networked AV** screen appears.

Figure 47 Wizard > Basic Settings > Step 3 Networked AV



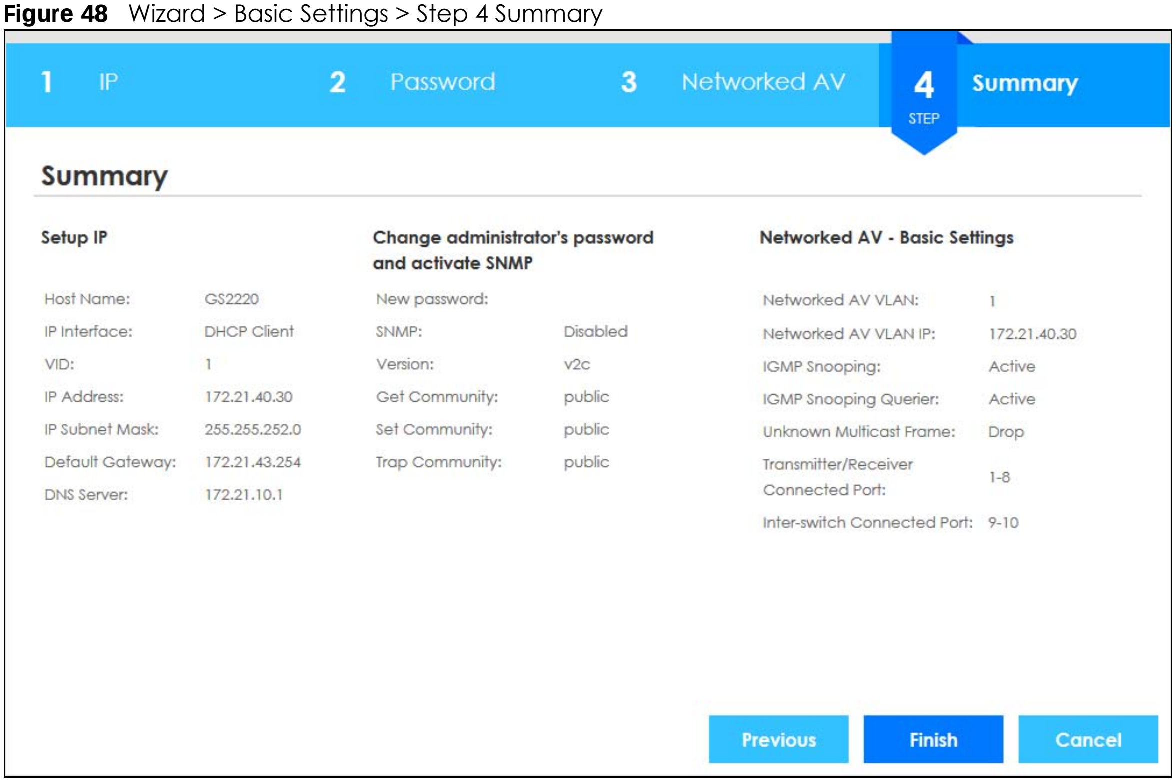
Each field is described in the following table.

Table 10 Wizard > Basic Settings > Step 3 Networked AV

LABEL	DESCRIPTION
Skip Networked AV Mode Settings	For the advanced user who do NOT wish to use the Switches' basic default AVoIP settings, click this option. Otherwise, just leave this unchecked and follow the diagram showing usage of the Switches' RJ45 ports for connecting to networked audio and video equipments, and the Combo or Fiber port for connecting to another switch. The **Inter-switch Connection** is used to connect to another switch. The combo or fiber ports will be aggregated automatically to increase bandwidth.
Previous	Click **Previous** to show the previous screen.
Next	Click **Next** to show the next screen.
Cancel	Click **Cancel** to exit this screen without saving.

After clicking **Next,** the **Summary** screen appears.

Figure 48 Wizard > Basic Settings > Step 4 Summary



Each field is described in the following table.

Table 11 Wizard > Basic Settings > Step 4 Summary

LABEL	DESCRIPTION
Setup IP	
Host Name	This field displays a host name.
IP Interface	This field displays whether the WAN interface is using a DHCP IP address or a static IP address.
VID	This field displays the VLAN ID.

Table 11 Wizard > Basic Settings > Step 4 Summary (continued)

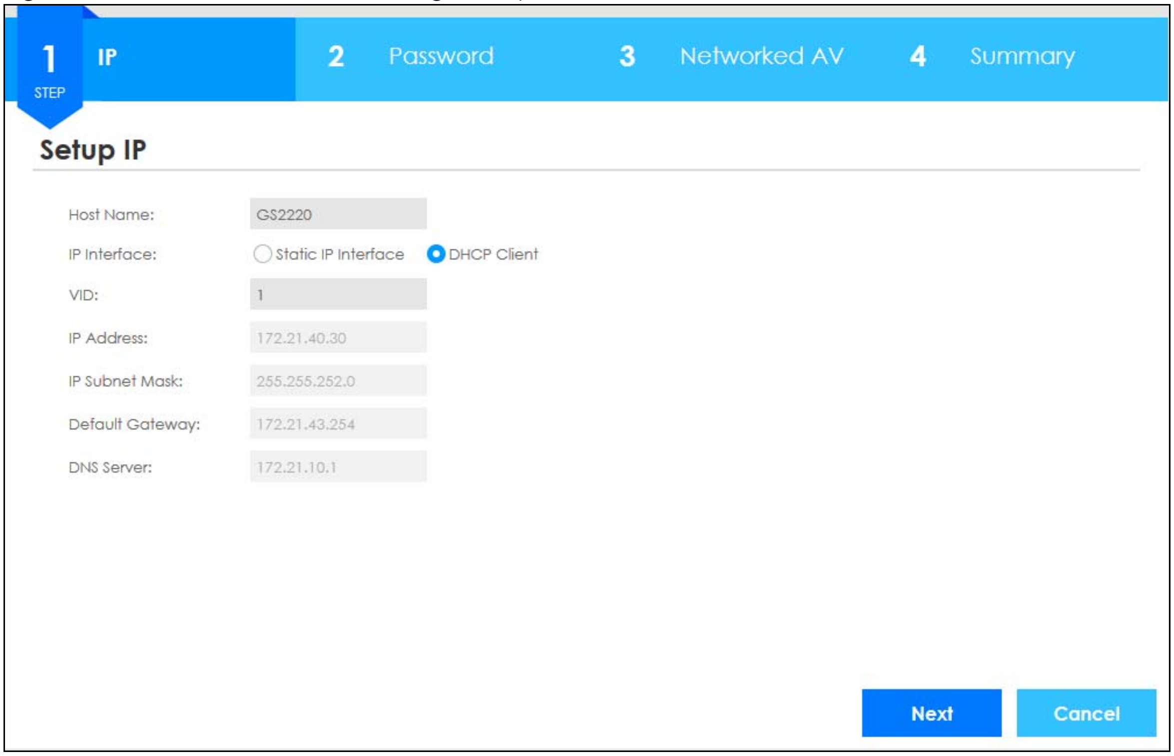
LABEL	DESCRIPTION
IP Address	This field displays the Switches' IP address for it to be managed over the network.
IP Subnet Mask	This field displays the subnet mask that specifies the network number portion of an IP address.
Default Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	This field displays the DNS (Domain Name System) for mapping a domain name to its corresponding IP address and vice versa.
Change administrator's password and activate SNMP	
New Password	This field displays asterisks when a new password has been created.
SNMP	This field displays whether the Switch acts as an SNMP agent.
Version	This field displays the SNMP version for the Switch.
Get Community	This field displays the **Get Community** string.
Set Community	This field displays the **Set Community** string.
Trap Community	This field displays the **Trap Community** string.
Networked AV – Basic Settings	
Networked AV VLAN	This field displays the VLAN ID for the AVoIP network.
Networked AV VLAN IP	This field displays the Switches' IP address for it to be managed over the AVoIP network.
IGMP Snooping	This field displays **Active** when IGMP Snooping is enabled to forward group multicast traffic only to ports that are members of that group. Otherwise, it displays **Inactive**.
IGMP Snooping Querier	This field displays **Active** when the Switch is allowed to send IGMP General Query messages to the VLANs with the multicast hosts attached. Otherwise, it displays **Inactive**.
Unknown Multicast Frame	This field displays the action to perform when the Switch receives an unknown multicast frame. It displays **Drop** when the frames are discarded. It displays **Flooding** when the frames are sent to all ports.
Transmitter/Receiver Connected Port	This field shows the Switches' port numbers for connection to networked audio and video equipment.
Inter-switch Connected Port	This field shows the Switches' port numbers for connection to another switch.
Previous	Click **Previous** to show the previous screen.
Finish	Review the information and click **Finish** to create the task.
Cancel	Click **Cancel** to exit this screen without saving.

4.4.2 Advanced Settings

In **Advanced Settings**, you can set up IP or DNS, set up your password, SNMP community, configure Networked AV service to a VLAN, select and assign port role, link aggregation (trunking), and view finished results.

In order to set up your IP or DNS, please do the following. Click **Wizard** > **Advanced Settings** > **Step 1 IP** to access this screen.

Figure 49 Wizard > Advanced Settings > Step 1 IP



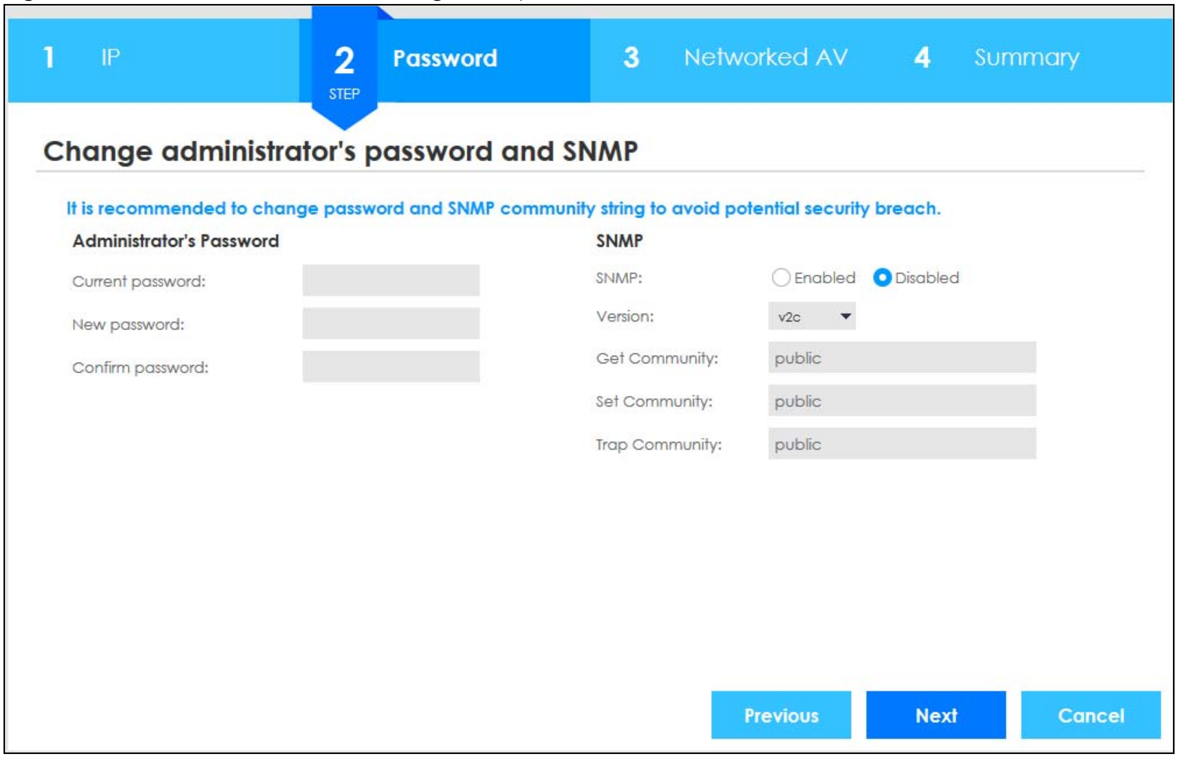
Each field is described in the following table.

Table 12 Wizard > Advanced Settings > Step 1 IP

LABEL	DESCRIPTION
Host Name	This field displays a host name.
IP Interface	Select **DHCP Client** if the Switch is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Switch in order to access the Switch's Web Configurator again. Select **Static IP Interface** when the Switch is NOT connected to a router or you want to assign it a fixed IP address.
VID	This field displays the VLAN ID.
IP Address	The Switch needs an IP address for it to be managed over the network.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Next	Click **Next** to show the next screen.
Cancel	Click **Cancel** to exit this screen without saving.

After clicking **Next,** the **Password** screen appears.

Figure 50 Wizard > Advanced Settings > Step 2 Password



Each field is described in the following table.

Table 13 Wizard > Advanced Settings > Step 2 Password

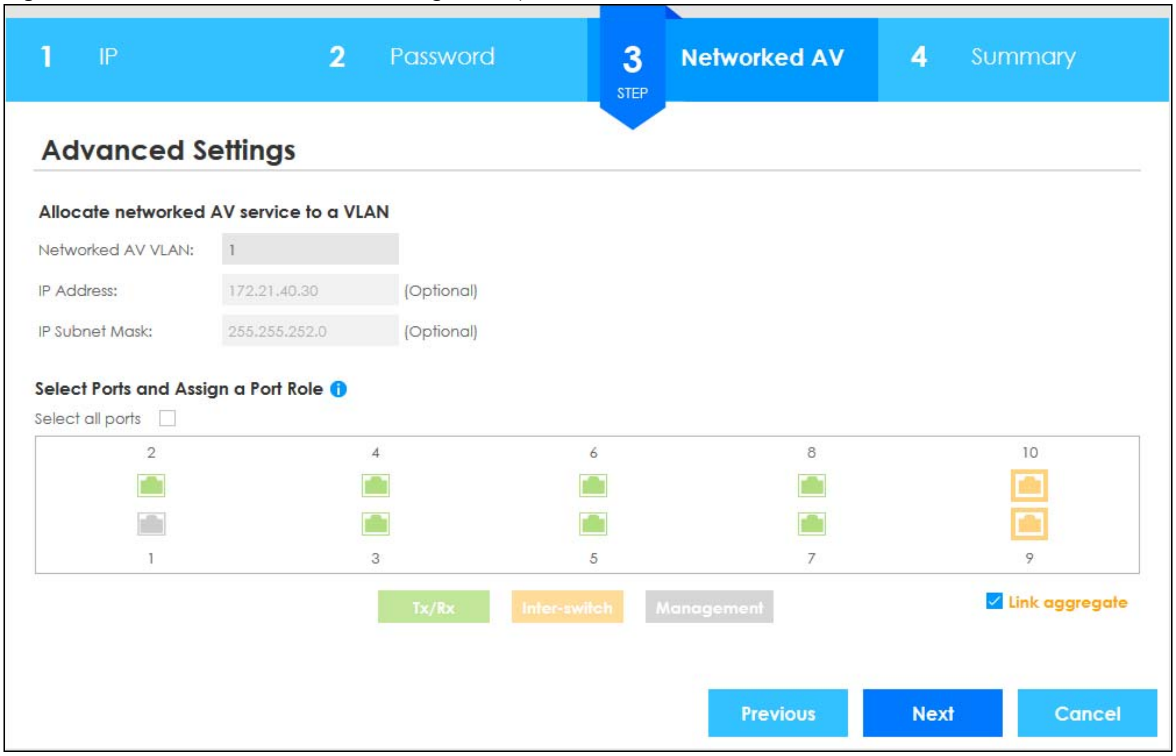
LABEL	DESCRIPTION
Administrator's Password	
Current password	Type the existing system password (1234 is the default password when shipped).
New password	Enter your new system password.
Confirm password	Retype your new system password for confirmation.
SNMP	
SNMP	Select **Enabled** to let the Switch act as an SNMP agent, which allows a manager station to manage and monitor the Switch through the network. Select **Disabled** to turn this feature off.
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 GetNextrequests 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.

Table 13   Wizard > Advanced Settings > Step 2 Password (continued)

LABEL	DESCRIPTION
Previous	Click **Previous** to show the previous screen.
Next	Click **Next** to show the next screen.
Cancel	Click **Cancel** to exit this screen without saving.

After clicking **Next**, the **Networked AV** screen appears.

Figure 51   Wizard > Advanced Settings > Step 3 Networked AV



Each field is described in the following table.

Table 14   Wizard > Advanced Settings > Step 3 Networked AV

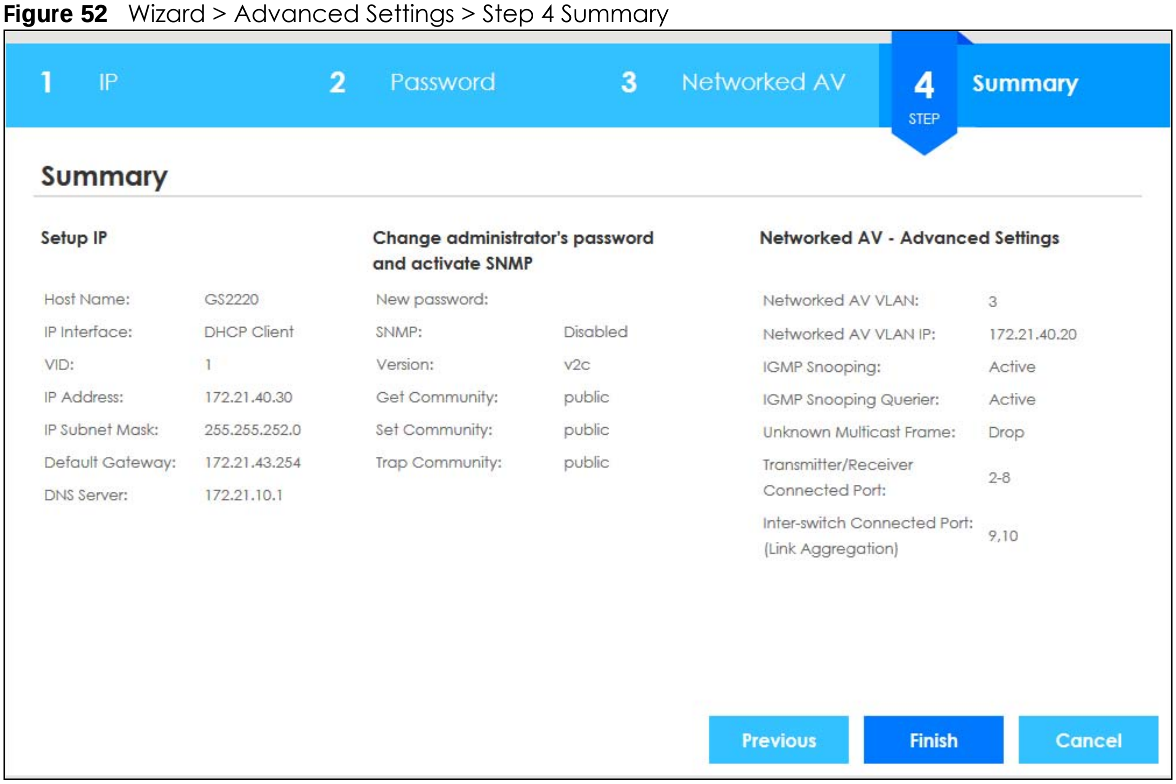
LABEL	DESCRIPTION
Allocate networked AV service to a VLAN	
Networked AV VLAN	Enter a number between 1 and 4094 to create a VLAN for the AVoIP network.
IP Address (Optional)	You must enter a different VLAN ID in the previous field (**Networked AV VLAN**) to be able to assign another IP address for the Switch to be managed over the AVoIP network.
IP Subnet Mask (Optional)	You must enter a different VLAN ID in the **Networked AV VLAN** field to be able to assign another subnet mask that specifies the network number portion of an IP address.
Select Ports and Assign a Port Role	

Table 14 Wizard > Advanced Settings > Step 3 Networked AV

LABEL	DESCRIPTION
Select all ports	After you create a VLAN, select the ports to be assigned to the Networked AV VLAN. **Select all ports** to assign the same role all ports. You can select a port by clicking it. Then click any of the following: Click **Tx/Rx** to assign the ports for connecting to networked audio and video equipments. Click **Inter-switch** to assign the ports for connecting to other switches. Click **Management** to reserve a port for administrative management if your Networked AV VLAN is different from management VLAN.
Link aggregate	Select this option to aggregate multiple port bandwidth if you are connecting to another switch. Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link.
Previous	Click **Previous** to show the previous screen.
Next	Click **Next** to show the next screen.
Cancel	Click **Cancel** to exit this screen without saving.

After clicking **Next,** the **Summary** screen appears.

Figure 52 Wizard > Advanced Settings > Step 4 Summary



Each field is described in the following table.

Table 15 Wizard > Advanced Settings > Step 4 Summary

LABEL	DESCRIPTION
Setup IP	
Host Name	This field displays a host name.

Table 15 Wizard > Advanced Settings > Step 4 Summary (continued)

LABEL	DESCRIPTION
IP Interface	This field displays whether the WAN interface is using a DHCP IP address or a static IP address.
VID	This field displays the VLAN ID.
IP Address	This field displays the Switches' IP address for it to be managed over the network.
IP Subnet Mask	This field displays the subnet mask that specifies the network number portion of an IP address.
Default Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	This field displays the DNS (Domain Name System) for mapping a domain name to its corresponding IP address and vice versa.
Change administrator's password and activate SNMP	
New Password	This field displays asterisks when a new password has been created.
SNMP	This field displays whether the Switch acts as an SNMP agent.
Version	This field displays the SNMP version for the Switch.
Get Community	This field displays the **Get Community** string.
Set Community	This field displays the **Set Community** string.
Trap Community	This field displays the **Trap Community** string.
Networked AV – Advanced Settings	
Networked AV VLAN	This field displays the VLAN ID for the AVoIP network.
Networked AV VLAN IP	This field displays the corresponding VLAN ID's IP address for the AVoIP network.
IGMP Snooping	This field displays **Active** when IGMP Snooping is enabled to forward group multicast traffic only to ports that are members of that group. Otherwise, it displays **Inactive**.
IGMP Snooping Querier	This field displays **Active** when the Switch is allowed to send IGMP General Query messages to the VLANs with the multicast hosts attached. Otherwise, it displays **Inactive**.
Unknown Multicast Frame	This field displays the action to perform when the Switch receives an unknown multicast frame. It displays **Drop** when the frames are discarded. It displays **Flooding** when the frames are sent to all ports.
Transmitter/Receiver Connected Port	This field shows the Switches' port numbers for connection to networked audio and video equipment.
Inter-switch Connected Port (Link Aggregation)	This field shows the Switches' port numbers for connection to another switch.
Previous	Click **Previous** to show the previous screen.
Finish	Review the information and click **Finish** to create the task.
Cancel	Click **Cancel** to exit this screen without saving.

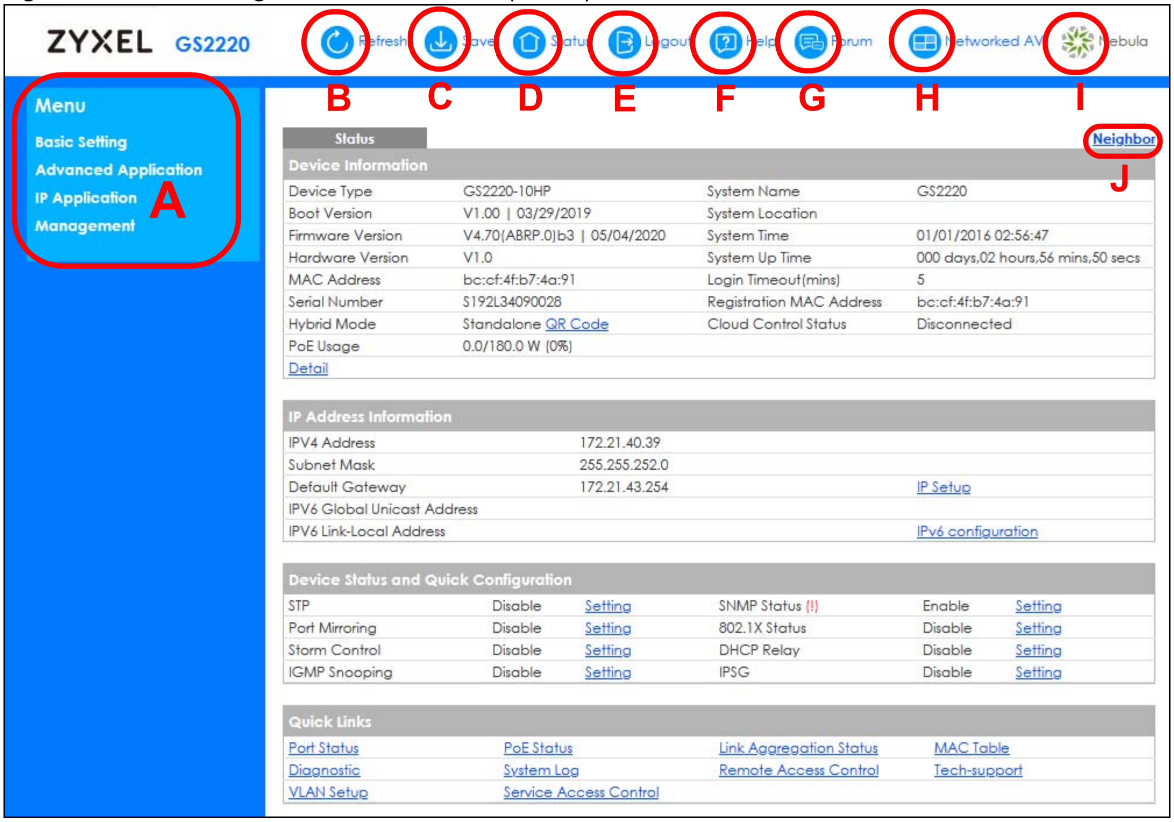
4.5 Web Configurator Layout

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

This guide uses GS2220-10HP screens as an example. The screens may very slightly for different models.

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

Figure 53 Web Configurator Home Screen (Status)



A – Click the menu items to open sub-menu links, and then click on a sub-menu 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 non-volatile memory. Non-volatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

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 Zyxel Community Biz Forum.

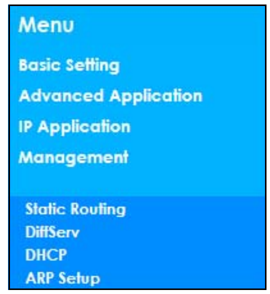
H – Click this icon to switch between the Web Configurator's **Standard** or **Networked AV** mode.

I – Click this link to go to the NCC (Nebula Control Center) portal website.

J – Click this link to go to the **Neighbor** 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 sub-menu links.

Table 16   Navigation Panel Sub-links Overview (Standard Mode)

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

The following table describes the links in the navigation panel.

Table 17   Navigation Panel Links (Standard Mode)

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address and subnet mask (necessary for Switch management) and set up to 64 IP routing domains.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.

Table 17 Navigation Panel Links (Standard Mode) (continued)

LINK	DESCRIPTION
PoE Setup	For PoE models. 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 configure settings for individual interface type and ID.
IPv6	This link takes you to a screen where you can view IPv6 status and configure IPv6 settings.
Cloud Management	This screen displays a link to a screen where you can enable or disable the **Nebula Control Center Discovery** feature. If it is enabled, you can have the Switch search for the NCC (Nebula Control Center). Another link takes you to the **Nebula Switch Registration** screen which has a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC.
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 voice VLAN, a MAC based VLAN or a vendor ID based VLAN in these screens.
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for ports. 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 to prevent network loops.
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the Switch.
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 screens 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 define different schedules.
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.
Multicast	This link takes you to screens where you can configure various multicast features and IGMP snooping.
AAA	This link takes you to a screen where you can configure authentication, authorization and accounting services via external servers. The external servers should be RADIUS (Remote Authentication Dial-In User Service).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.

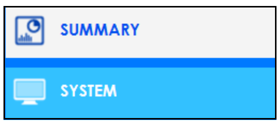
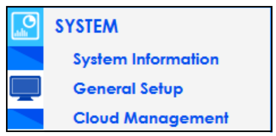
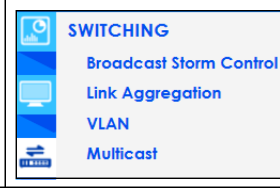
Table 17 Navigation Panel Links (Standard Mode) (continued)

LINK	DESCRIPTION
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.
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 screens where you can view errdisable status and configure errdisable settings in CPU protection, errdisable detect, and errdisable recovery.
Vlan Isolation	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 green Ethernet settings in EEE, auto power down, and short reach for each port.
LLDP	This link takes you to screens 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 settings.
Auto PD Recovery	For PoE models. This link takes you to a screen where you can enable and configure Auto PD Recovery on the Switch.
IP Application	
Static Routing	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
ARP Setup	This link takes you to screens where you can configure the ARP learning settings for each port.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to a screen where you can ping IP addresses, run traceroute, test ports and show the Switch's location.
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 screens 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 addresses (and types) of devices attached to what ports and VLAN IDs.

Table 17   Navigation Panel Links (Standard Mode) (continued)

LINK	DESCRIPTION
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Path MTU Table	This link takes you to a screen where you can view the path MTU aging time, index, destination address, MTU, and expire settings.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to other ports.
IPv6 Neighbor Table	This link takes you to a screen where you can view the IPv6 neighbor table which includes index, interface, neighbor address, MAC address, status and type.
Port Status	This link takes you to a screen where you can view the port statistics.

Table 18   Navigation Panel Sub-links Overview (Networked AV Mode)

SUMMARY	SYSTEM	PORT	SWITCHING
			

NETWORKING	SECURITY	MAINTENANCE
		

Table 19   Navigation Panel Links (Networked AV Mode)

LINK	DESCRIPTION
Summary	This screen displays the Switch's front panel port status, connected ports, used power, Nebula Cloud Control status, and Networked AV status.
SYSTEM	
System Information	This link takes you to a screen that displays general system information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Cloud Management	This screen displays a link to a screen where you can enable or disable the **Nebula Control Center Discovery** feature. If it is enabled, you can have the Switch search for the NCC (Nebula Control Center). Another link takes you to the **Nebula Switch Registration** screen which has a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC.
PORT	

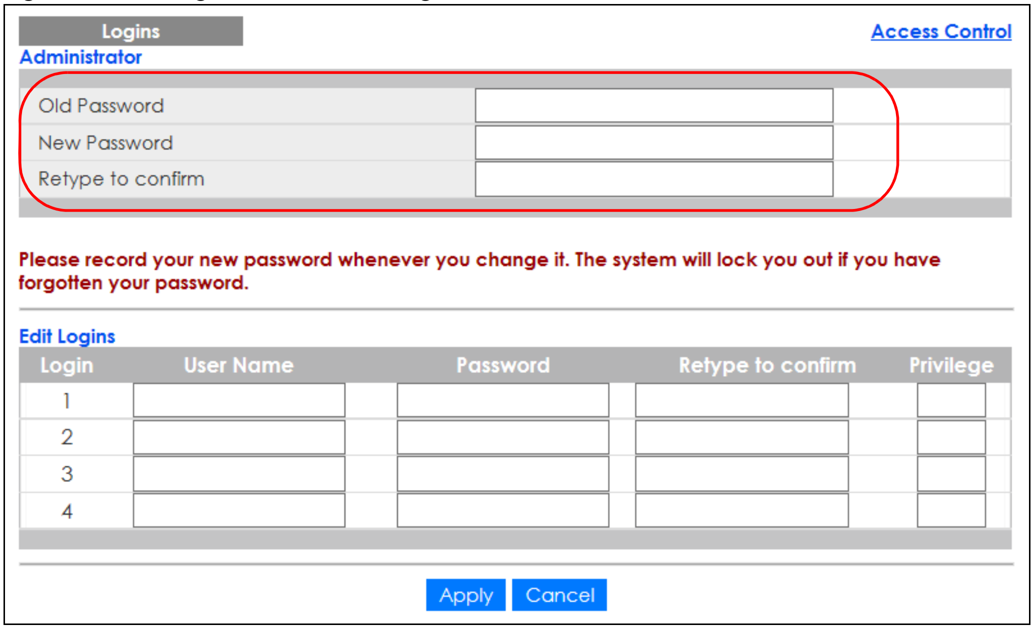
Table 19 Navigation Panel Links (Networked AV Mode) (continued)

LINK	DESCRIPTION
PoE Setup	For PoE models. This screen allows you to set priorities, PoE power-up settings and schedule so that the Switch is able to reserve and allocate power to certain PDs.
Port Setup	This screen allows you to configure settings for individual Switch ports.
SWITCHING	
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Link Aggregation	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
VLAN	This link takes you to screens where you can view and search all static VLAN groups, view detailed port settings and status of the static VLAN group, configure a static VLAN for the Switch, and configure the static VLAN (IEEE 802.1Q) settings on a port.
Multicast	This link takes you to screens where you can view multicast group information, configure various multicast features like IGMP snooping and filtering profile, and create multicast VLANs.
NETWORKING	
IP Setup	This screen allows you to configure the IP address and subnet mask (necessary for Switch management) and set up to 64 IP routing domains.
SECURITY	
Access Control	
Logins	This link takes you to a screen where you can change the system login password, as well as configure up to four login details.
Remote Management	This link takes you to a screen where you can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
SNMP	This link takes you to screens where you can specify the SNMP version and community (password) values, configure where to send SNMP traps from the Switch, enable loopguard/errdisable/poe/linkup/linkdown/lldp/transceiver-ddm/storm-control on the Switch, specify the types of SNMP traps that should be sent to each SNMP manager, and add/edit user information.
Service Access Control	This link takes you to a screen where you can decide what services you may use to access the Switch.
Maintenance	
Backup Configuration	This link takes you to a screen where you can save your Switch's configurations (settings) for later use.
Firmware Upgrade	This link takes you to a screen to upload firmware to your Switch.
Reboot System	This link takes you to a screen to reboot the Switch without turning the power off.
Restore Configuration	This link takes you to a screen where you can upload a stored device configuration file.
Save Configuration	This link takes you to a screen where you can save the current configuration (settings) to a specific configuration file on the Switch.
Tech-Support	This link takes you to a screen where you can download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.
Port Mirror	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.

4.5.1 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 54 Change Administrator Login Password



4.6 Save 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 non-volatile memory. Non-volatile 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.

4.7 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.

9 You forgot to log out of the Switch from a computer before logging in again on another computer.

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.

4.8 Reset 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.

4.8.1 Restore Button

Press the **RESTORE** button for more than 7 seconds to have the Switch automatically reboot and restore the factory default file. See Section 3.3 on page 47 for more information about the LED behavior. See also Table 3 on page 40 to see how to use the **RESTORE** button to restore the factory default file.

4.8.2 Restore Custom Default

Press the **RESTORE** button for 3 to 7 seconds to have the Switch automatically reboot and restore the last-saved custom default file. See Section 3.3 on page 47 for more information about the LED behavior.

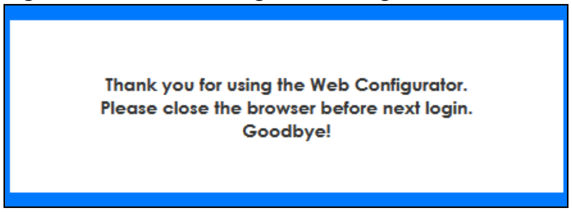
4.8.3 Reboot the Switch

Press the **RESET** button to reboot the Switch without turning the power off. See Section 3.3 on page 47 for more information about the LED behavior.

4.9 Log 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 55 Web Configurator: Logout Screen



4.10 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.

CHAPTER 5
Initial Setup Example

5.1 Overview

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

The following lists the configuration steps for the initial setup:

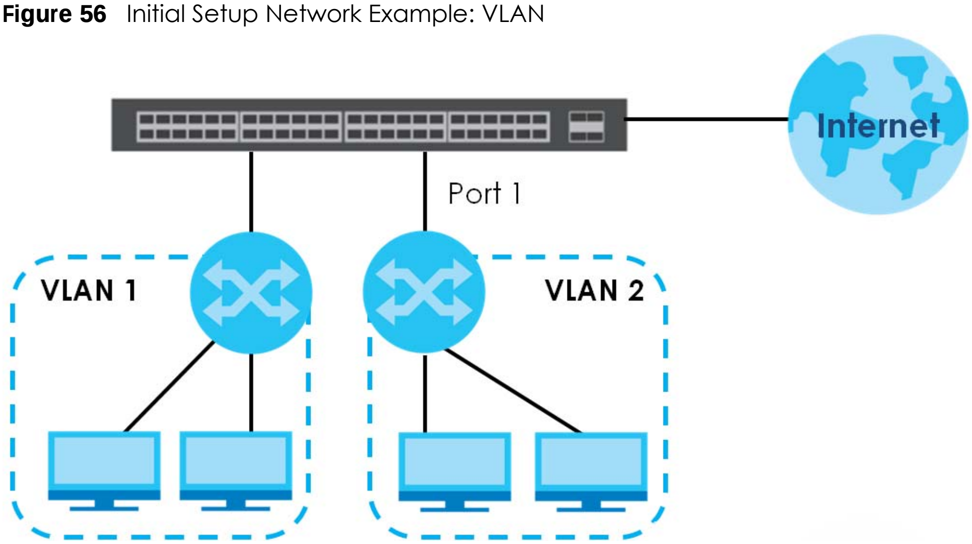
- Create a VLAN
- Set Port VID
- Configure Switch Management IP Address

5.1.1 Create a VLAN

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

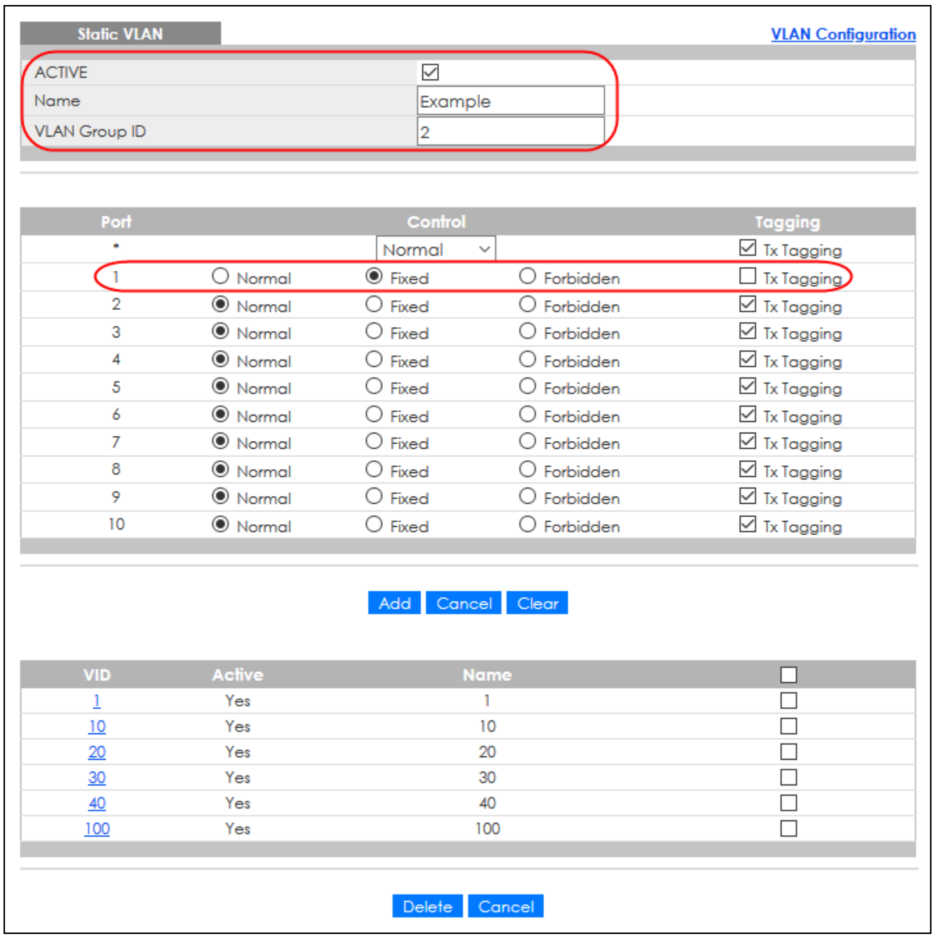
In this example, you want to configure port 1 as a member of VLAN 2.

Figure 56 Initial Setup Network Example: VLAN



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

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



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

3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.

4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

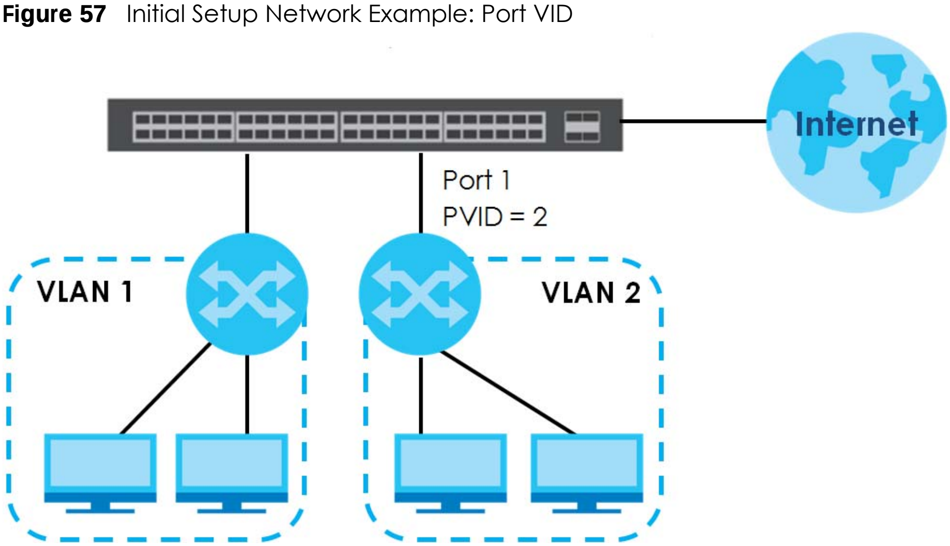
5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.2 Set Port VID

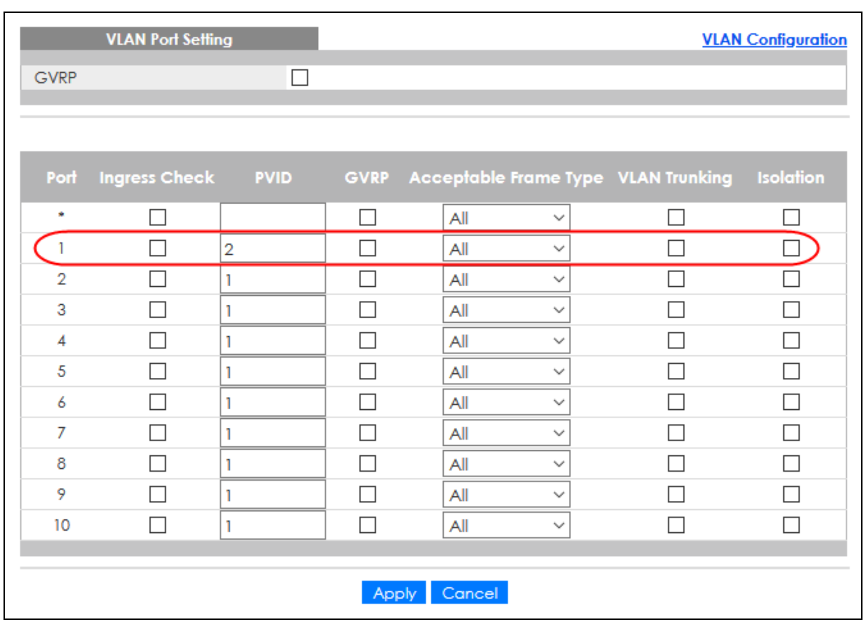
Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

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

Figure 57 Initial Setup Network Example: Port VID



1 Click **Advanced Application** > **VLAN** > **VLAN Configuration** in the navigation panel. Then click the **VLAN Port Setup** link.

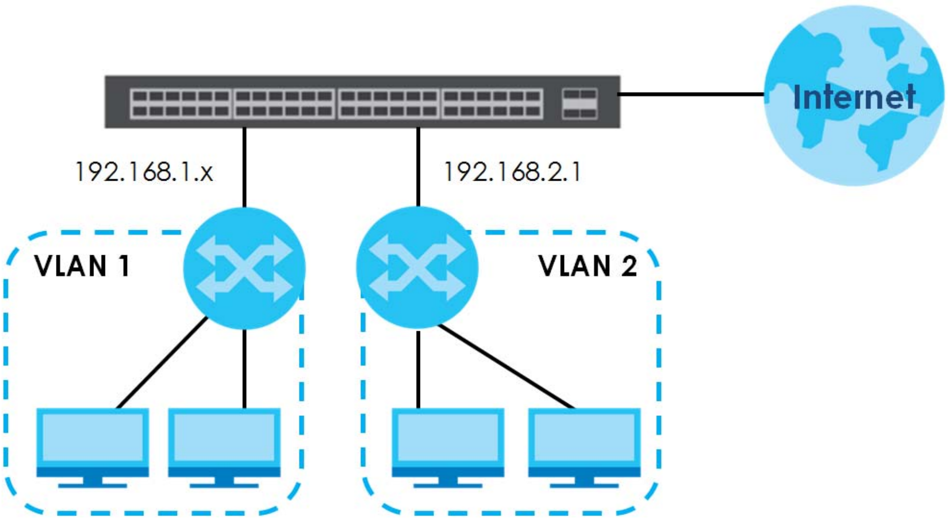


2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.3 Configure Switch Management IP Address

If the Switch fails to obtain an IP address from a DHCP server, the Switch will use 192.168.1.1 as the management IP address. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

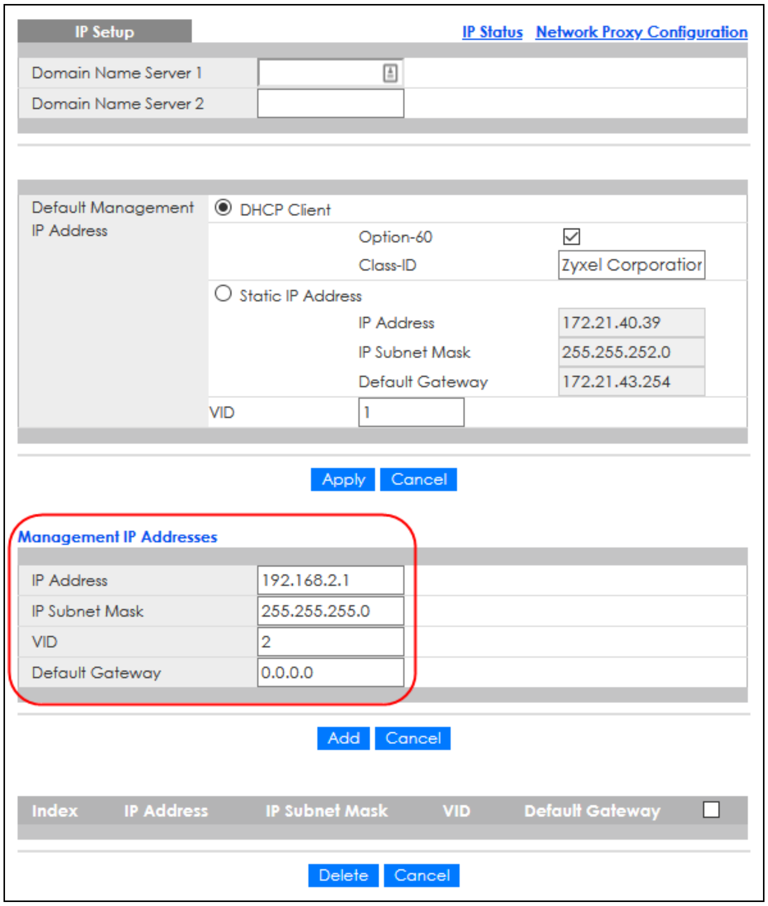
Figure 58 Initial Setup Example: Management IP Address



1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.

2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the Web Configurator. See Section 4.2 on page 50 for more information.

3 Click **Basic Setting** > **IP Setup** > **IP Configuration** in the navigation panel.



4 Configure the related fields in the **IP Setup** screen.

5 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

6 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.

7 Click **Add** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

CHAPTER 6 Tutorials

6.1 Overview

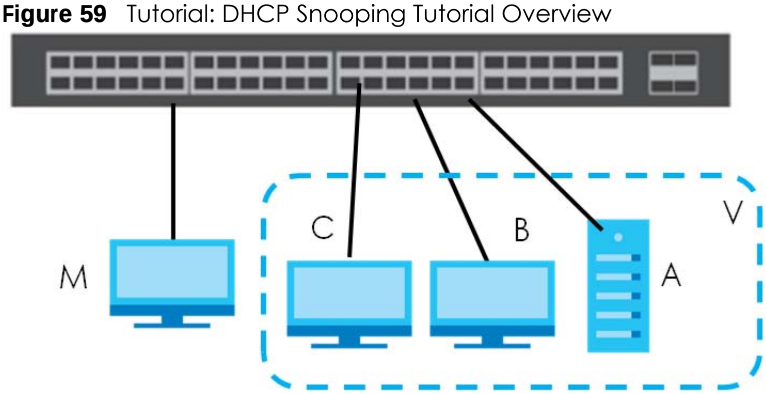
This chapter provides some examples of using the Web Configurator to set up and use the Switch. The tutorials include:

- How to Use DHCPv4 Snooping on the Switch
- How to Use DHCPv4 Relay on the Switch
- How to Use Auto Configuration via a DHCP Server on the Switch

6.2 How to Use DHCPv4 Snooping on the Switch

You only want DHCP server **A** connected to port 4 to assign IP addresses to all devices in VLAN network (**V**). Create a VLAN containing ports 4, 5 and 6. Connect a computer **M** to the Switch for management.

Figure 59 Tutorial: DHCP Snooping Tutorial Overview



The settings in this tutorial are as the following.

Table 20 Tutorial: Settings in this Tutorial

HOST	PORT CONNECTED	VLAN	PVID	DHCP SNOOPING PORT TRUSTED
DHCP Server (**A**)	4	1 and 100	100	Yes
DHCP Client (**B**)	5	1 and 100	100	No
DHCP Client (**C**)	6	1 and 100	100	No

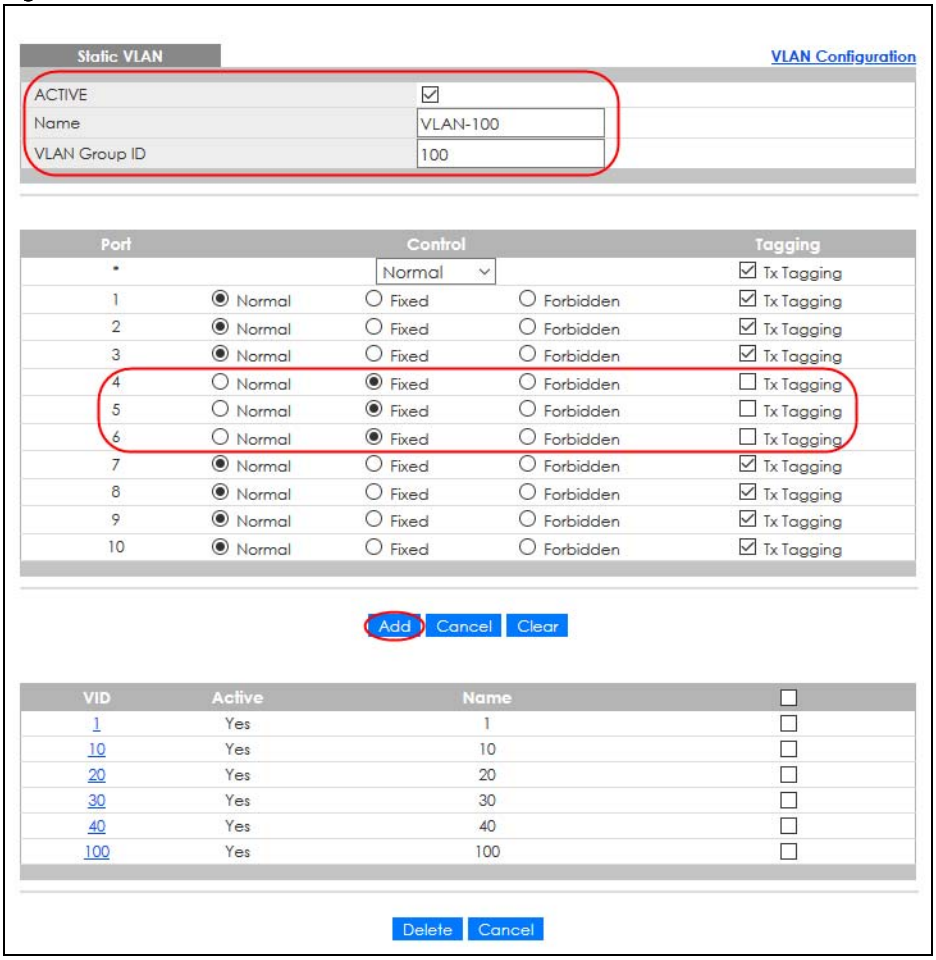
1 Access the Switch through **http://192.168.1.1** by default. Log into the Switch by entering the user name (default: **admin**) and password (default: **1234**).

2 Go to **Advanced Application** > **VLAN** > **VLAN Configuration** > **Static VLAN Setup**, and create a VLAN with ID of 100. Add ports 4, 5 and 6 in the VLAN by selecting **Fixed** in the **Control** field as shown.

De-select **Tx Tagging** because you do not want outgoing traffic to contain this VLAN tag.

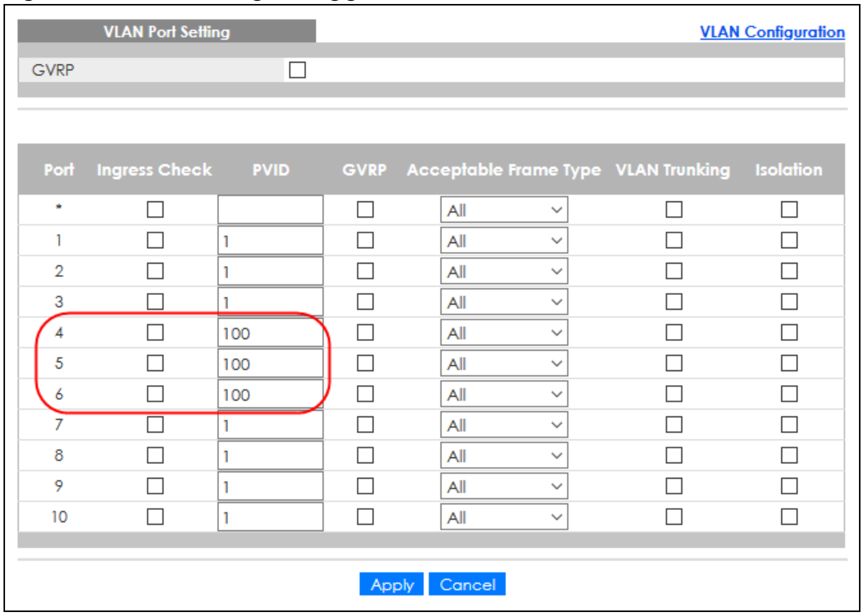
Click **Add**.

Figure 60 Tutorial: Create a VLAN and Add Ports to It



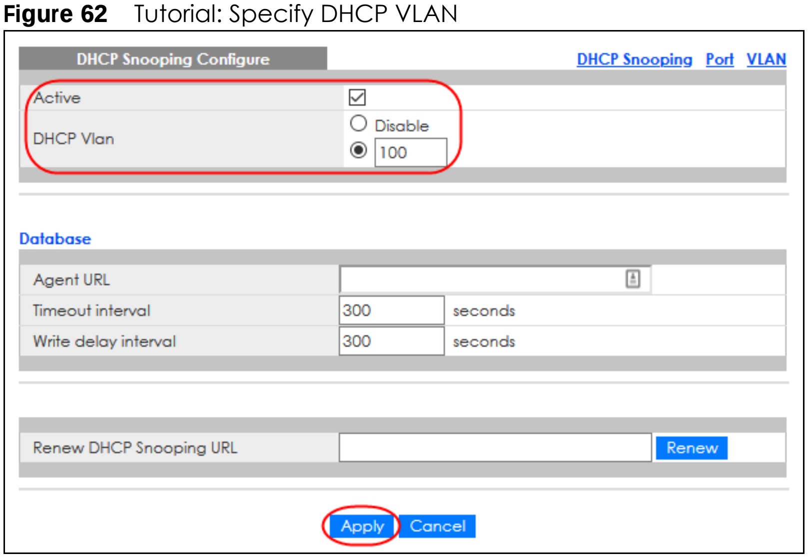
3 Go to **Advanced Application** > **VLAN** > **VLAN Configuration** > **VLAN Port Setup**, and set the PVID of the ports 4, 5 and 6 to 100. This tags untagged incoming frames on ports 4, 5 and 6 with the tag 100.

Figure 61   Tutorial: Tag Untagged Frames



4 Go to **Advanced Application** > **IP Source Guard** > **IPv4 Source Guard Setup** > **DHCP Snooping** > **Configure**, activate and specify VLAN 100 as the DHCP VLAN as shown. Click **Apply**.

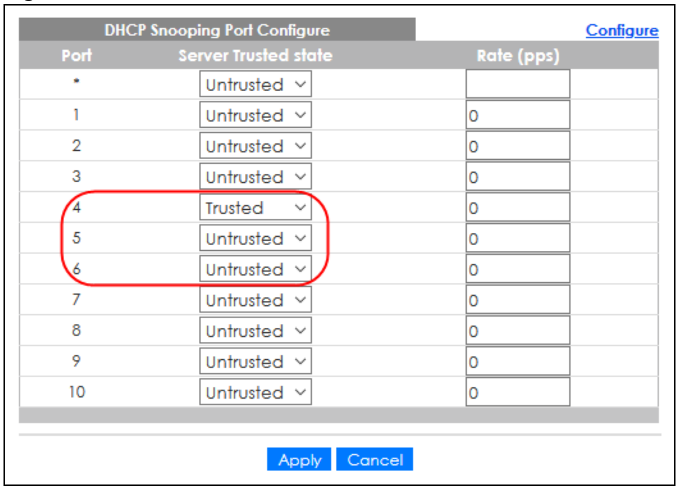
Figure 62   Tutorial: Specify DHCP VLAN



5 Click the **Port** link at the top right corner.

6 The **DHCP Snooping Port Configure** screen appears. Select **Trusted** in the **Server Trusted state** field for port 4 because the DHCP server is connected to port 4. Keep ports 5 and 6 **Untrusted** because they are connected to DHCP clients. Click **Apply**.

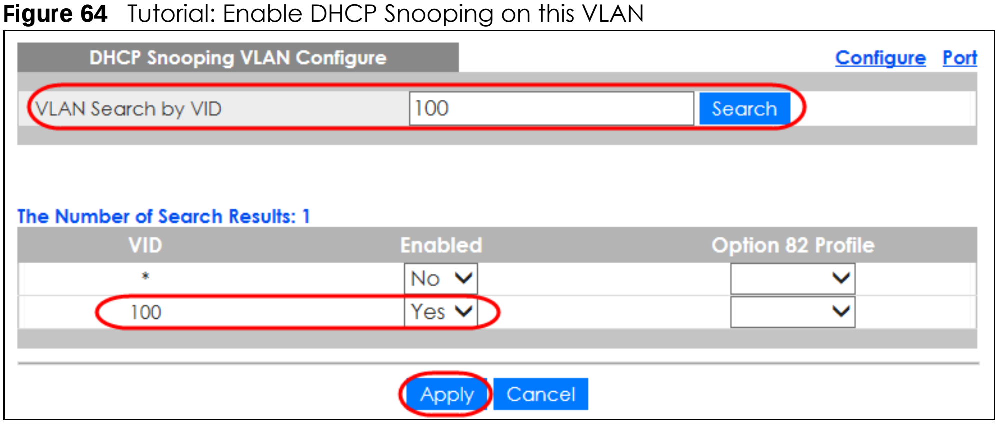
Figure 63 Tutorial: Set the DHCP Server Port to Trusted



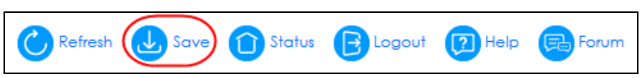
7 Go to **Advanced Application** > **IP Source Guard** > **IPv4 Source Guard Setup** > **DHCP Snooping** > **Configure** > **VLAN**, show VLAN 100 by entering 100 in the **Start VID** and **End VID** fields and click **Apply**. Then select **Yes** in the **Enabled** field of the VLAN 100 entry shown at the bottom section of the screen.

If you want to add more information in the DHCP request packets such as source VLAN ID or system name, you can also select an **Option82 Profile** in the entry.

Figure 64 Tutorial: Enable DHCP Snooping on this VLAN



8 Click **Save** at the top right corner of the Web Configurator to save the configuration permanently.



9 Connect your DHCP server to port 4 and a computer (as DHCP client) to either port 5 or 6. The computer should be able to get an IP address from the DHCP server. If you put the DHCP server on port 5 or 6, the computer will NOT be able to get an IP address.

10 To check if DHCP snooping works, go to **Advanced Application** > **IP Source Guard** > **IPv4 Source Guard Setup**, you should see an IP assignment with the type **DHCP-Snooping** as shown.

Figure 65 Tutorial: Check the Binding If DHCP Snooping Works

IP Source Guard — IPSG | Static Binding | DHCP Snooping | ARP Inspection

Index	IP Address	VLAN	MAC Address	Port	Lease	Type
1	10.10.1.16	100	00:02:00:00:00:1c	6	6d23h17m 0s	dchp-snooping

You can also telnet. Use the command "`show dhcp snooping binding`" to see the DHCP snooping binding table as shown next.

```
sysname# show dhcp snooping binding
        MacAddress          IpAddress          Lease           Type  VLAN   Port
  -----------------  ---------------  ------------  -------------  ----  -----
  00:02:00:00:00:1c       10.10.1.16   6d23h59m20s  dhcp-snooping   100      6
  Total number of bindings: 1
```

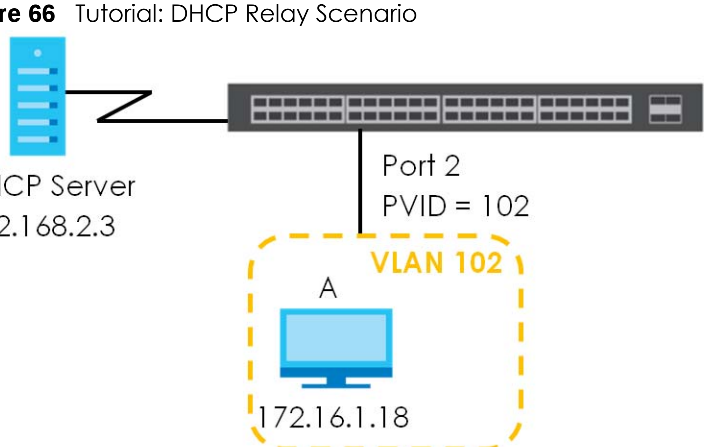
6.3 How to Use DHCPv4 Relay on the Switch

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

6.3.1 DHCP Relay Tutorial Introduction

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

Figure 66 Tutorial: DHCP Relay Scenario

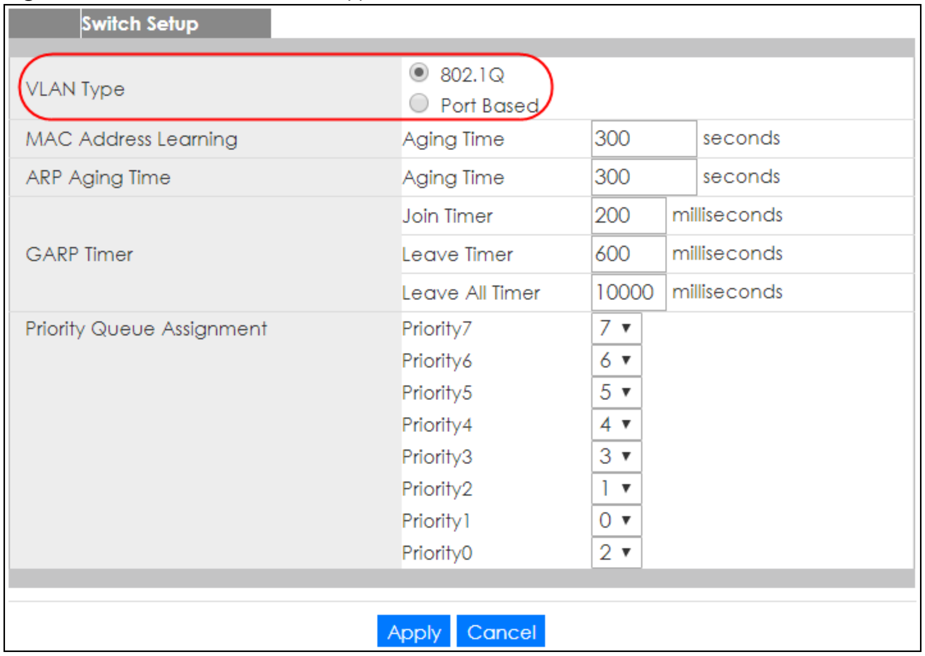


6.3.2 Create a VLAN

Follow the steps below to configure port 2 as a member of VLAN 102.

1. Access the Web Configurator through the Switch's management port.
2. Go to **Basic Setting** > **Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.

Figure 67 Tutorial: Set VLAN Type to 802.1Q



3 Click **Advanced Application** > **VLAN** > **VLAN Configuration** > **Static VLAN Setup**.

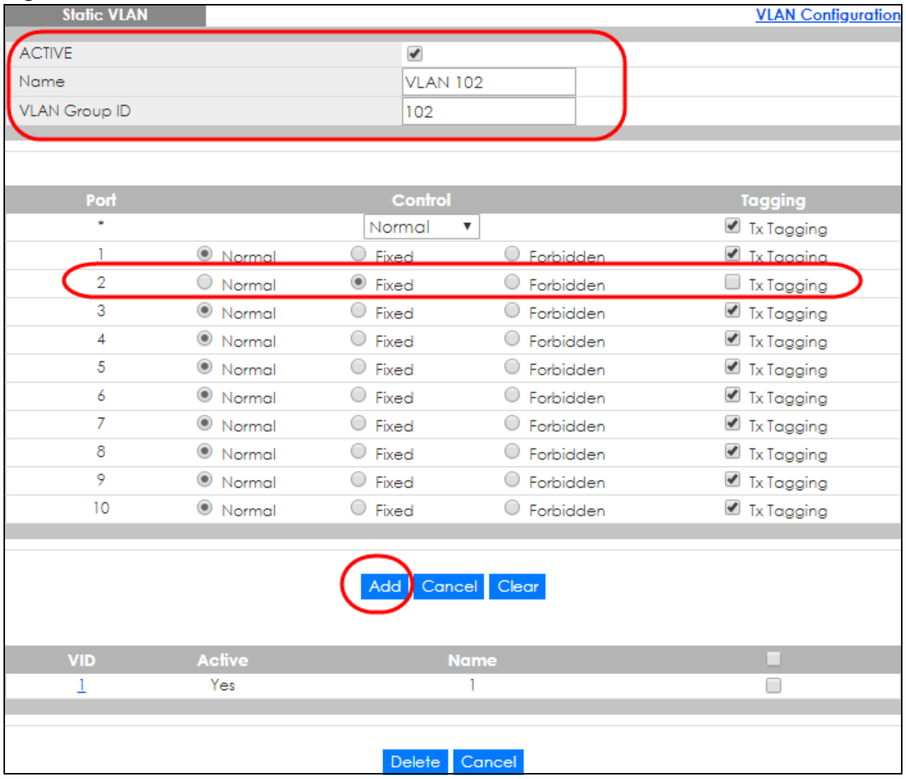
4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 102 for example) in the **Name** field and enter 102 in the **VLAN Group ID** field.

5 Select **Fixed** to configure port 2 to be a permanent member of this VLAN.

6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

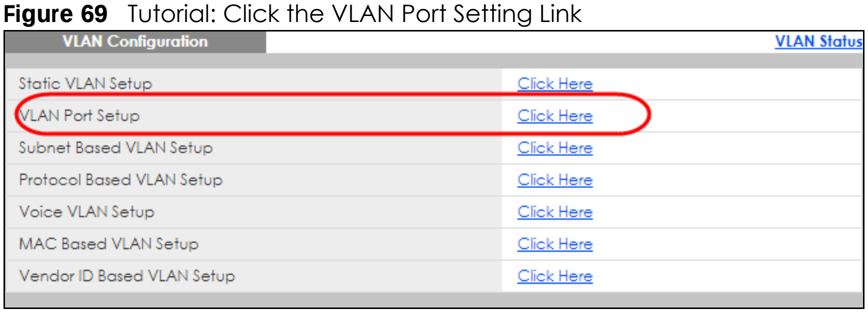
7 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Figure 68 Tutorial: Create a Static VLAN



8 Click the **VLAN Configuration** link in the **Static VLAN Setup** screen and then the **VLAN Port Setup** link in the **VLAN Configuration** screen.

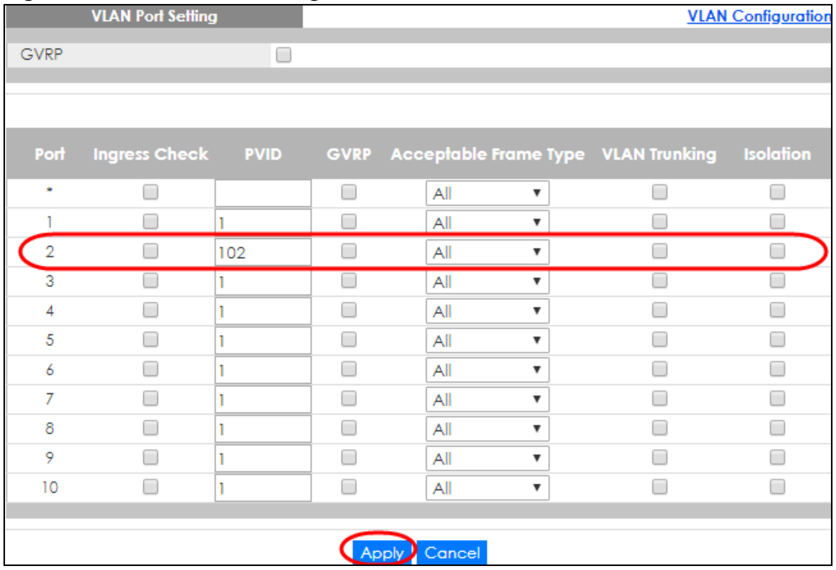
Figure 69 Tutorial: Click the VLAN Port Setting Link



9 Enter 102 in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

10 Click **Apply** to save your changes back to the run-time memory.

Figure 70 Tutorial: Add Tag for Frames Received on Port 2



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

6.3.3 Configure DHCPv4 Relay

Follow the steps below to enable DHCP relay on the Switch and allow the Switch to add relay agent information (such as the VLAN ID) to DHCP requests.

1 Click **IP Application** > **DHCP** > **DHCPv4** and then the **Global** link to open the **DHCP Relay** screen.

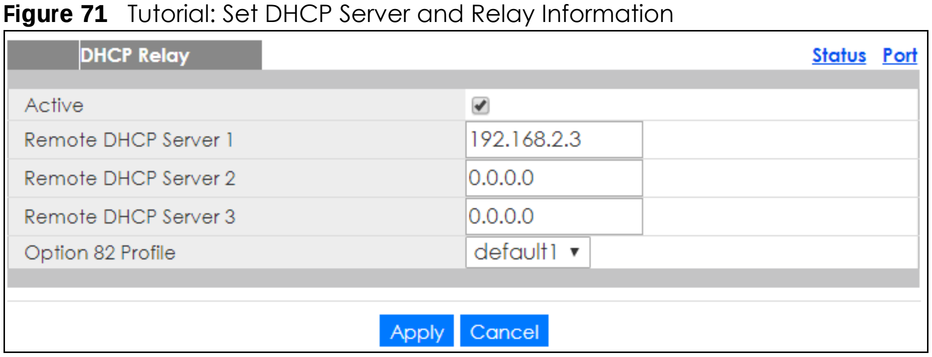
2 Select the **Active** check box.

3 Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.

4 Select **default1** or **default2** in the **Option 82 Profile** field.

5 Click **Apply** to save your changes back to the run-time memory.

Figure 71 Tutorial: Set DHCP Server and Relay Information



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

7 The DHCP server can then assign a specific IP address based on the DHCP request.

6.3.4 Troubleshooting

Check the client **A**'s IP address. If it did not receive the IP address 172.16.1.18, make sure:

1 Client **A** is connected to the Switch's port 2 in VLAN 102.

2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.

You clicked the **Save** link on the Switch to have your settings take effect.

6.4 How to Use Auto Configuration via a DHCP Server on the Switch

Follow the steps below to set up configurations on a DHCP server, TFTP server, and the Switch, so you can load an auto configuration file automatically from a TFTP server when you reboot the Switch.

Note that you can set up a DHCP server and TFTP server either on the same device or different devices. Also, make sure the Switch can communicate with the TFTP server.

Note: Steps order could vary according to different programs you use.

Note: You need to set up configurations on a DHCP server and TFTP server first to use auto configuration.

Setting up a DHCP Server

1 Set up a dynamic IP addresses pool so the DHCP server will assign an IP address to the Switch in that range.

2 Set up a TFTP server IP address, so the Switch will know where to load the auto configuration file.

3 Set up the filename of the auto configuration file, so the Switch will know which file to load when you reboot the Switch.

- Enter the filename of an auto configuration file. The Switch will load this auto configuration file when rebooting with DHCP option 60 disabled.
- If you want to load the auto configuration file with DHCP option 60 enabled and a Vendor Class Identifier assigned when you reboot the Switch, follow the instruction below. Otherwise, skip this step.
  Enter the filename of the an auto configuration file. Set up a Vendor Class Identifier. To have the Switch load this auto configuration file, two conditions listed above must be met. Please refer to the following steps to see how to set up a Vendor Class Identifier on the Switch.

Setting up a TFTP Server

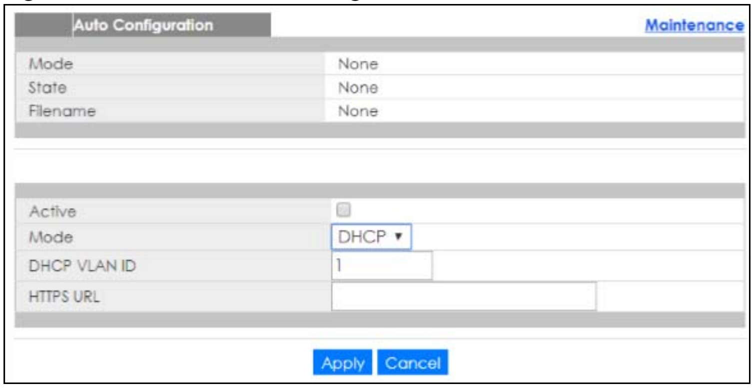
1 Select a directory on the TFTP server.

2 Put the configuration files in that directory.

Setting up the Switch

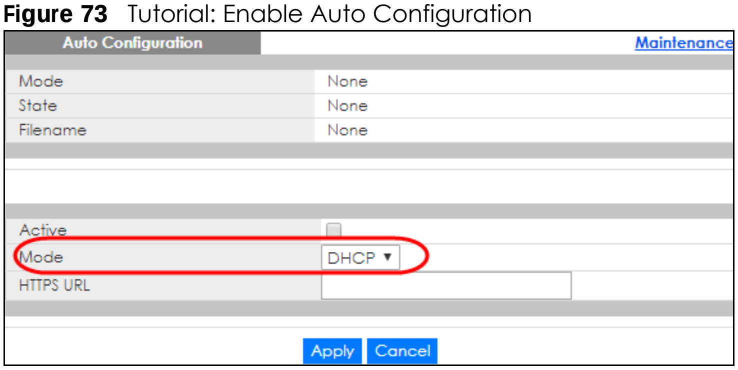
1 Open the Web Configurator. Go to the **Management** > **Maintenance** screen, and click the **Click Here** button next to the **Auto Configuration** field.

Figure 72 Tutorial: Auto Configuration Screen



2 Select the check box in the **Active** field to enable auto configuration. Select **DHCP** in the **Mode** field and click **Apply** to save your changes.

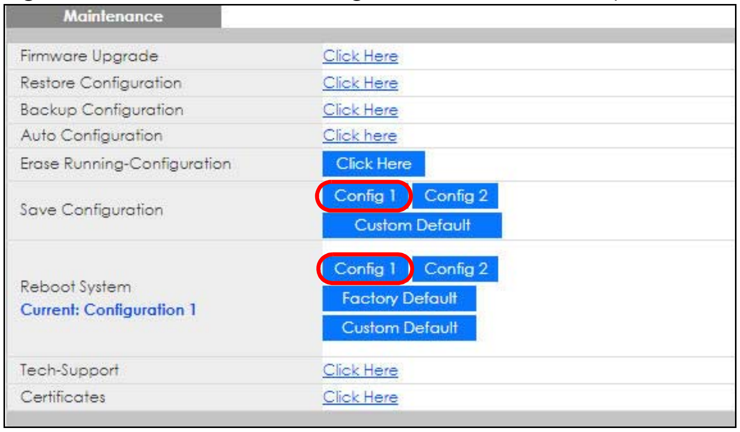
Figure 73 Tutorial: Enable Auto Configuration



3 You need to save the current configuration in a configuration file, so the Switch will load the auto configuration file from the TFTP server automatically when rebooting. Go to the **Management** > **Maintenance** screen. Click the **Config 1**, **Config2**, or **Custom Default** button next to the **Save Configuration** field. See Section 46.2 on page 392 for more information.

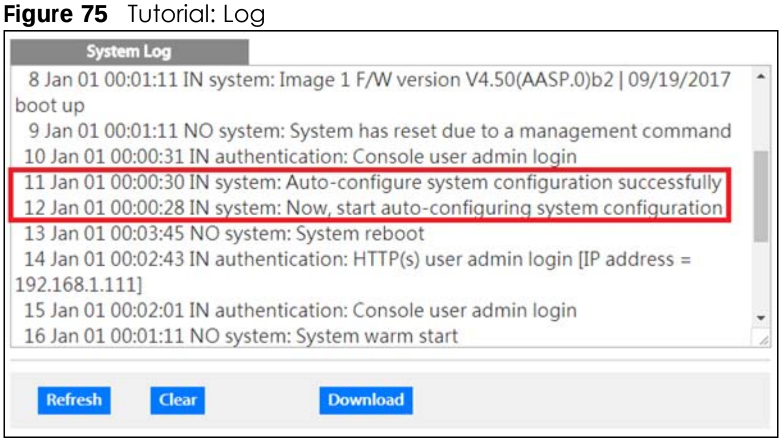
4 Click the same button next to **Reboot System** field to reboot the Switch, and load the auto configuration setting as configured before. For example, if you save the auto configuration setting to **Config 1**, you need to click the **Config 1** button next to the **Reboot System** field.

Figure 74 Tutorial: Save Configuration and Reboot System



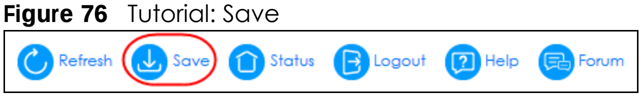
5 Go to the **Management** > **System Log** screen to see if auto configuration was performed successfully.

Figure 75 Tutorial: Log



6 Check the screens to see if it is the configuration file you want to load. If it is not, go through the steps above to check your configurations. If it is, click **Save** at the top right corner of the Web Configurator to save the configuration permanently.

Figure 76 Tutorial: Save



CHAPTER 7
Status

7.1 Overview

This chapter describes the screens for System Status and Neighbor Details.

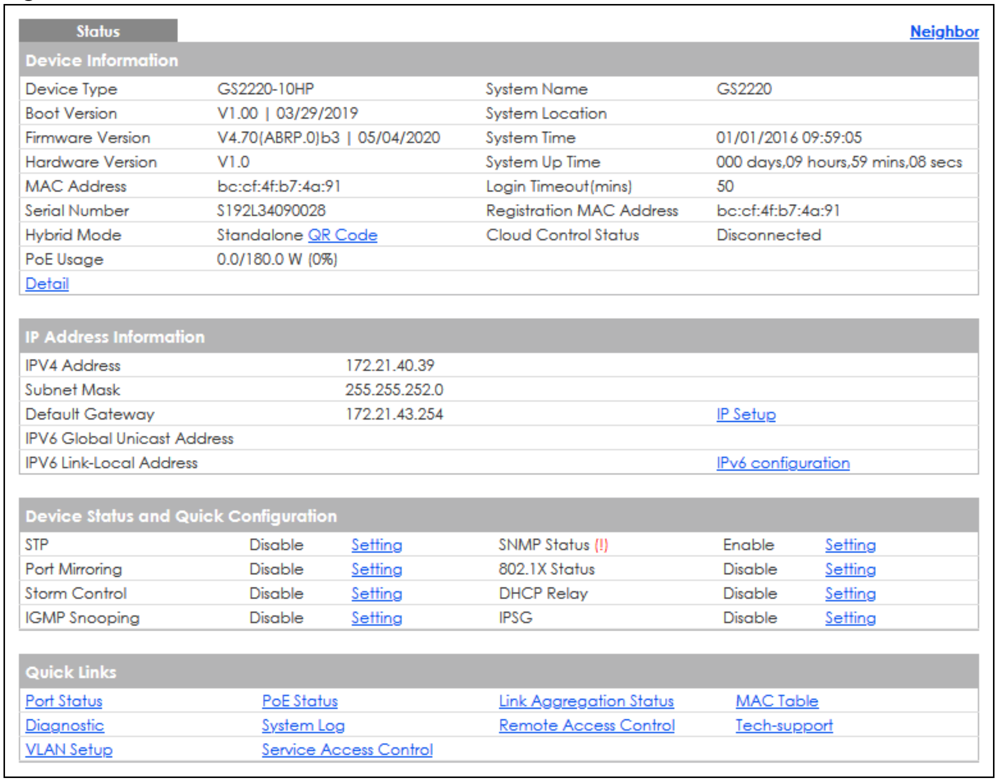
7.1.1 What You Can Do

- Use the **Status** screen (Section 7.2 on page 94) to see the Switch's general device information, system status, and IP addresses. You can also display other status screens for more information.
- Use the **Neighbor** screen (Section 7.2.1 on page 96) to view a summary and manage Switch's neighbor devices.
- Use the **Neighbor Detail** screen (Section 7.2.2 on page 98) to view more detailed information on the Switch's neighbor devices.

7.2 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 77 Status



The following table describes the labels in this screen.

Table 21 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.
Hardware Version	This field displays the hardware version number of the Switch. The integer is the generation number of the Switch series, and the decimal is the version of the hardware change. For example, V1.0 is a hardware version for the Switch where 1 identifies the first generation of the Switch series, and .0 is the first hardware change.
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(mins)	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.
Serial Number	This field displays the serial number of this Switch. The serial number is used for device tracking and control.
Registration MAC Address	This field displays the MAC address of the Switch that you must use to register at myZyxel.com or the NCC (Nebula Control Center).

Table 21 Status (continued)

LABEL	DESCRIPTION
Hybrid Mode	This field displays whether the Switch is in **Standalone** mode or **Cloud** mode. In **Standalone** mode you can see a link to a QR code to register the Switch to use NCC (Nebula Control Center).
Cloud Control Status	This field displays the registration and connection status between the Switch and the NCC (Nebula Control Center). In Standalone mode, the status will display **Disconnected** or **Unregistered**. In cloud mode the status will display **Connected** or **Disconnected**. **Connected** – The Switch is registered with and connected to the NCC. **Disconnected** – The Switch is not connected to the NCC. **Unregistered** – The Switch is not registered with the NCC.
PoE Usage	This field displays the amount of power the Switch is currently supplying to the connected PoE-enabled devices and the total power the Switch can provide to the connected PDs. It also shows the percentage of PoE power usage. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in **Basic Setting** > **PoE Setup**.
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.
Quick Links	This section provides the shortcut link to a specific configuration screen.

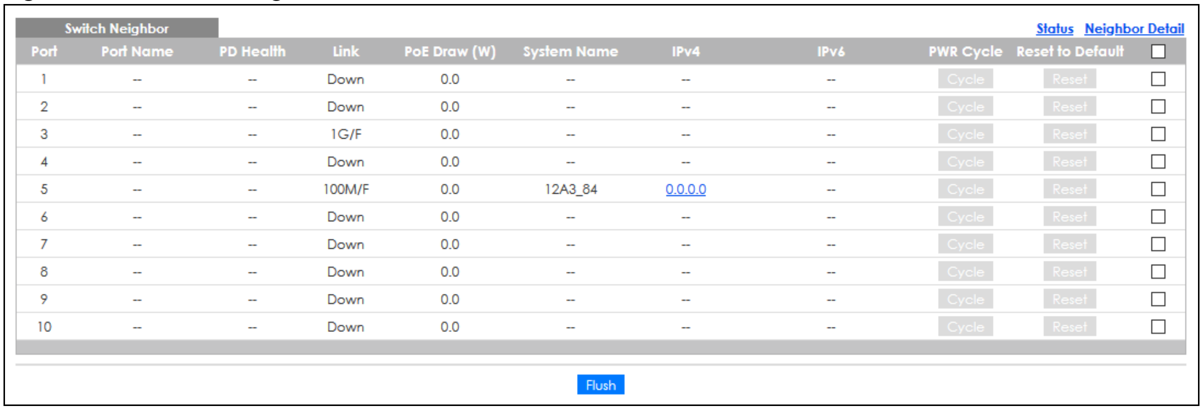
7.2.1 Neighbor Screen

The **Neighbor** screen allows you to view a summary and manage the Switch's neighboring devices. It uses Layer Link Discovery Protocol (LLDP) to discover all neighbor devices connected to the Switch including non-Zyxel devices. You can use this screen to perform tasks on the neighboring devices like login, power cycle (turn the power off and then back on again), and reset to factory default settings.

This screen shows the neighboring device first recognized on an Ethernet port of the Switch. Device information is displayed in gray when the neighboring device is offline.

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

Figure 78 Status > Neighbor



The following table describes the fields in the above screen.

Table 22 Status > Neighbor

LABEL	DESCRIPTION
Port	This shows the port of the Switch, on which the neighboring device is discovered.
Port Name	This shows the port description of the Switch.
PD Health	This shows the status of auto PD recovery on this port. • Red: The Switch failed to get information from the PD connected to the port using LLDP, or the connected PD did not respond to the Switch's ping requests. • Yellow: The Switch is restarting the connected PD by turning the power off and turning it on again. • Green: The Switch successfully discovered the connected PD using LLDP or ping. • **–**: Auto PD Recovery is not enabled on the Switch and the port, or the Switch does not supply power to the connected PD. Note: The status will NOT be updated instantaneously after enabling or disabling the **Active** switch in the **Advanced Application** > **Auto PD Recovery** screen. It will wait until the configured **Resume Polling Interval (sec)** has lapsed.
Link	This shows the speed (either **10M** for 10Mbps, **100M** for 100Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half). This field displays **Down** if the port is not connected to any device.
PoE Draw (W)	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.
System Name	This shows the system name of the neighbor device.
IPv4	This shows the IPv4 address of the neighbor device. The IPv4 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
IPv6	This shows the IPv6 address of the neighbor device. The IPv6 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
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).

Table 22 Status > Neighbor (continued)

LABEL	DESCRIPTION
Reset to Default	Click the **Reset** button to reset the neighboring 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). • If multiple neighbor devices use the same port, the **Reset** button is not available. • You can only reset Zyxel powered devices that support the ZON utility.
	Select an entry's check box to select a specific port. Otherwise, select the check box in the table heading row to select all ports.
Flush	Click the **Flush** button to remove information about neighbors learned on the selected ports.

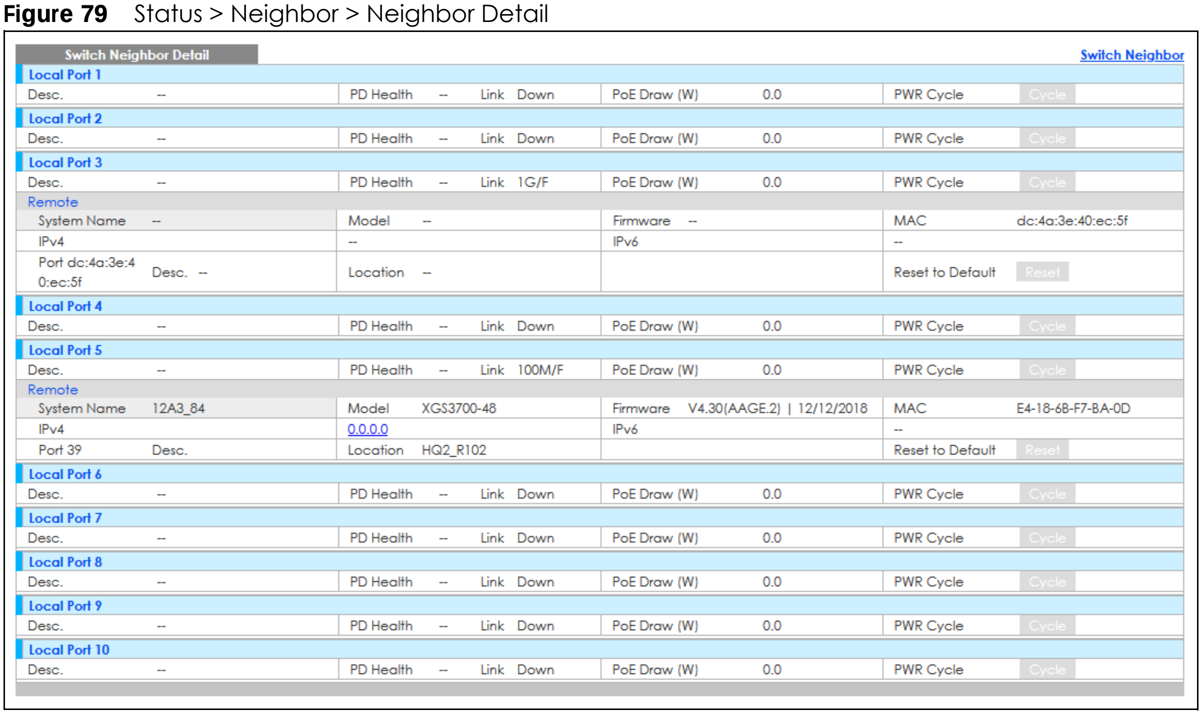
7.2.2 Neighbor Detail

Use this screen to view detailed information about the neighboring devices. Device information is displayed in gray when the neighboring device is currently offline.

Up to 10 neighboring device records per Ethernet port can be retained in this screen even when the devices are offline. When the maximum number of neighboring device records per Ethernet port is reached, new device records automatically overwrite existing offline device records, starting with the oldest existing offline device record first.

Click the **Neighbor Detail** link in the **Status** > **Neighbor** screen to see the following screen.

Figure 79 Status > Neighbor > Neighbor Detail



The following table describes the fields in the above screen.

Table 23 Status > Neighbor > Neighbor Detail

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.
PD Health	This shows the status of auto PD recovery on this port. • Red: The Switch failed to get information from the PD connected to the port using LLDP, or the connected PD did not respond to the Switch's ping requests. • Yellow: The Switch is restarting the connected PD by turning the power off and turning it on again. • Green: The Switch successfully discovered the connected PD using LLDP or ping. • **–**: Auto PD Recovery is not enabled on the Switch and the port, or the Switch does not supply power to the connected PD.
Link	This shows the speed (either **10M** for 10Mbps, **100M** for 100Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half). This field displays **Down** if the port is not connected to any device.
PoE Draw (W)	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.
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).
Remote	
System Name	This shows the system name of the neighbor device.
Model	This shows the model name of the neighbor device. This field will show "**–**" for devices that do not support the ZON utility.
Firmware	This shows the firmware version of the neighbor device. This field will show "**–**" for devices that do not support the ZON utility.
MAC	This shows the MAC address of the neighbor device.
IPv4	This shows the IPv4 address of the neighbor device. The IPv4 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
IPv6	This shows the IPv6 address of the neighbor device. The IPv6 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
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.
Location	This shows the geographic location of the neighbor device. This field will show "**–**" for devices that do not support the ZON utility.
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). • If multiple neighbor devices use the same port, the **Reset** button is not available. • You can only reset Zyxel powered devices that support the ZON utility.

CHAPTER 8
Basic Setting

8.1 Overview

This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup**, **Port Setup**, **PoE Setup**, **Interface Setup**, **IPv6**, and **Cloud Management** screens.

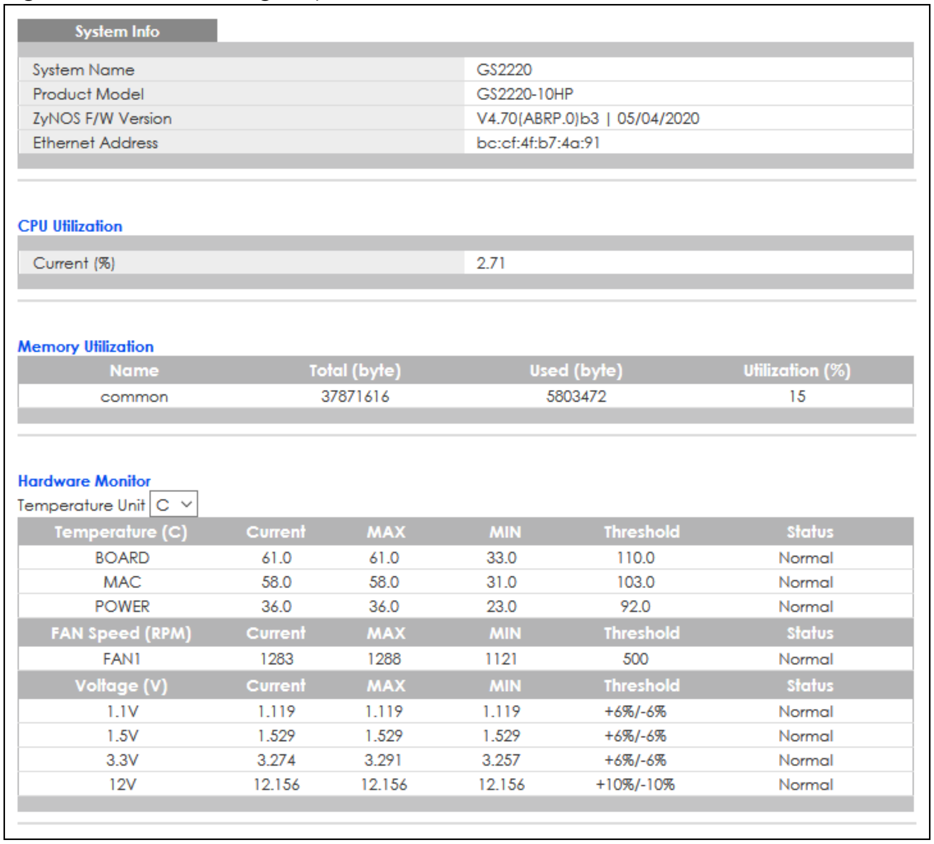
8.1.1 What You Can Do

- Use the **System Info** screen (Section 8.2 on page 100) to check the firmware version number and monitor the Switch temperature.
- Use the **General Setup** screen (Section 8.3 on page 102) to configure general settings such as the system name and time.
- Use the **Switch Setup** screen (Section 8.5 on page 105) to choose your VLAN type and assign priorities to queues.
- Use the **IP Setup** screen (Section 8.6 on page 106) to configure the Switch IP address, default gateway device, management VLAN ID, and proxy server.
- Use the **Port Setup** screen (Section 8.7 on page 111) to configure Switch port settings.
- Use the **PoE Setup** screens (Section 8.8 on page 113) to view the current amount of power that PDs are receiving from the Switch and set the priority levels for the Switch in distributing power to PDs. This screen is available for PoE models only.
- Use the **Interface Setup** screens (Section 8.9 on page 119) to configure Switch interface type and interface ID settings.
- Use the **IPv6** screens (Section 8.10 on page 120) to view IPv6 status and IPv6 configuration.
- Use the **Cloud Management** screen (Section 8.11 on page 131) to display links to **Nebula Control Center Discovery** and **Nebula Switch Registration** screens.

8.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. Use this screen to view general system information.

Figure 80 Basic Setting > System Info



The following table describes the labels in this screen.

Table 24 Basic Setting > System Info

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 (byte)	This field displays the total number of bytes in this memory pool.
Used (byte)	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	
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.

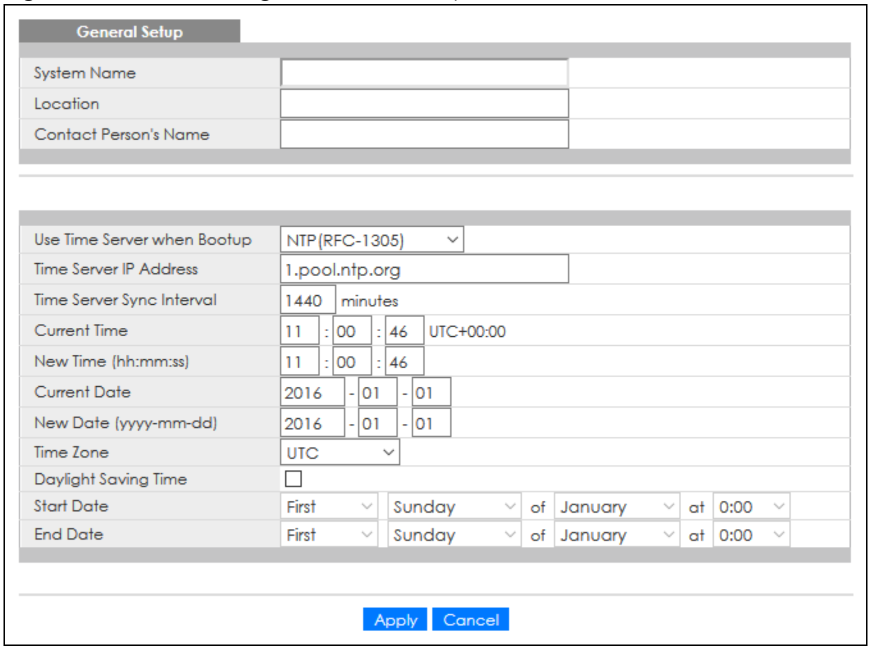
Table 24 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Temperature (C/F)	**BOARD** / **MAC** / **PHY** (**POWER** – for GS2220-10HP only) refers to the location of the temperature sensor 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 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.

8.3 General Setup

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

Figure 81 Basic Setting > General Setup



The following table describes the labels in this screen.

Table 25 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Enter the time service protocol that your time server 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 0:0:0.
Time Server IP Address	Enter the IP address or domain name of your timeserver. The Switch searches for the timeserver for up to 60 seconds.
Time Server Sync Interval	Enter the period in minutes between each time server synchronization. The Switch checks the time server after every synchronization interval.
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.

Table 25 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
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 first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **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).
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.

8.4 Introduction to VLANs

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

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

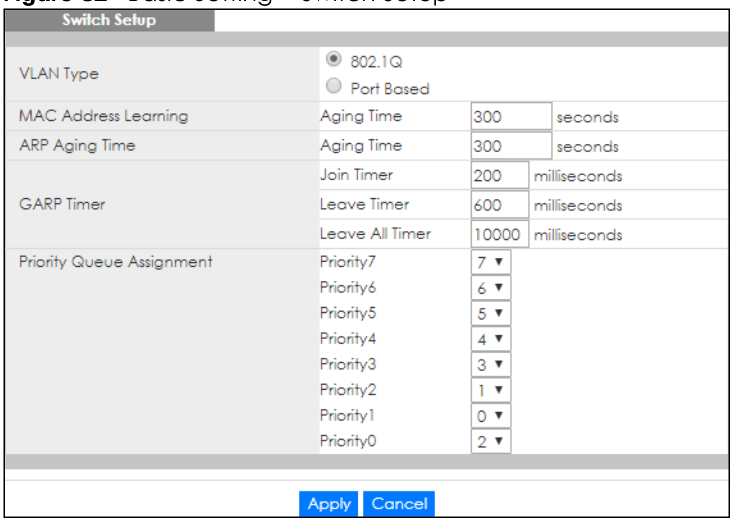
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

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

8.5 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.

Figure 82 Basic Setting > Switch Setup



The following table describes the labels in this screen.

Table 26 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	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.
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 the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup 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.

Table 26   Basic Setting > Switch Setup (continued)

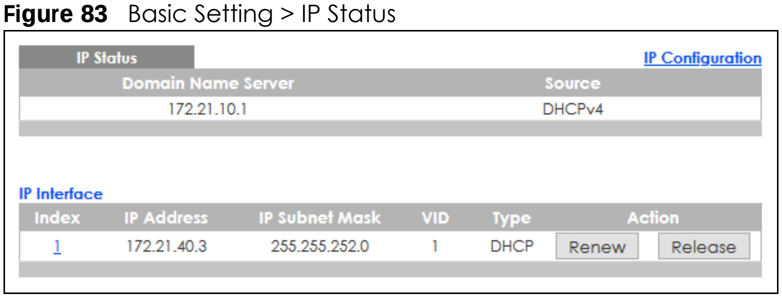
LABEL	DESCRIPTION
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the eight 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). To map a priority level to a physical queue, select a physical queue from the drop-down menu on the right.	
Priority 7	Typically used for network control traffic such as router configuration messages.
Priority 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Priority 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Priority 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Priority 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Priority 2	This is for "spare bandwidth".
Priority 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.
Priority 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.

8.6 IP Setup

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

8.6.1 IP Status

Figure 83   Basic Setting > IP Status



The following table describes the labels in this screen.

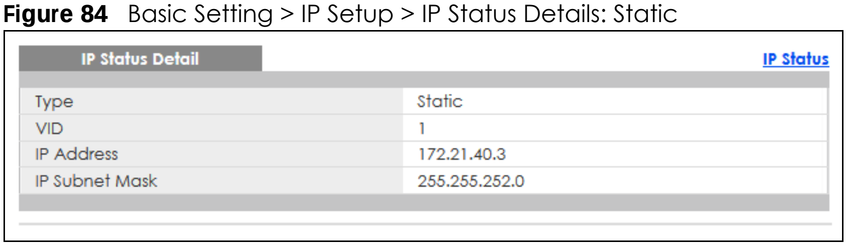
Table 27 Basic Setting > IP Status

LABEL	DESCRIPTION
IP Status	
Domain Name Server	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 **DHCPv4**.
IP Interface	
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.

8.6.2 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 84 Basic Setting > IP Setup > IP Status Details: Static

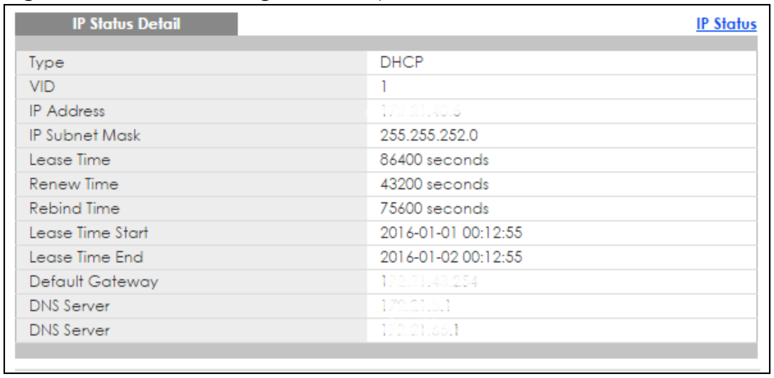


The following table describes the labels in this screen.

Table 28 Basic Setting > IP Setup > IP Status Details: Static

LABEL	DESCRIPTION
Type	This shows the IP address is manually assigned (**Static**).
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 85 Basic Setting > IP Setup > IP Status Details: DHCP



The following table describes the labels in this screen.

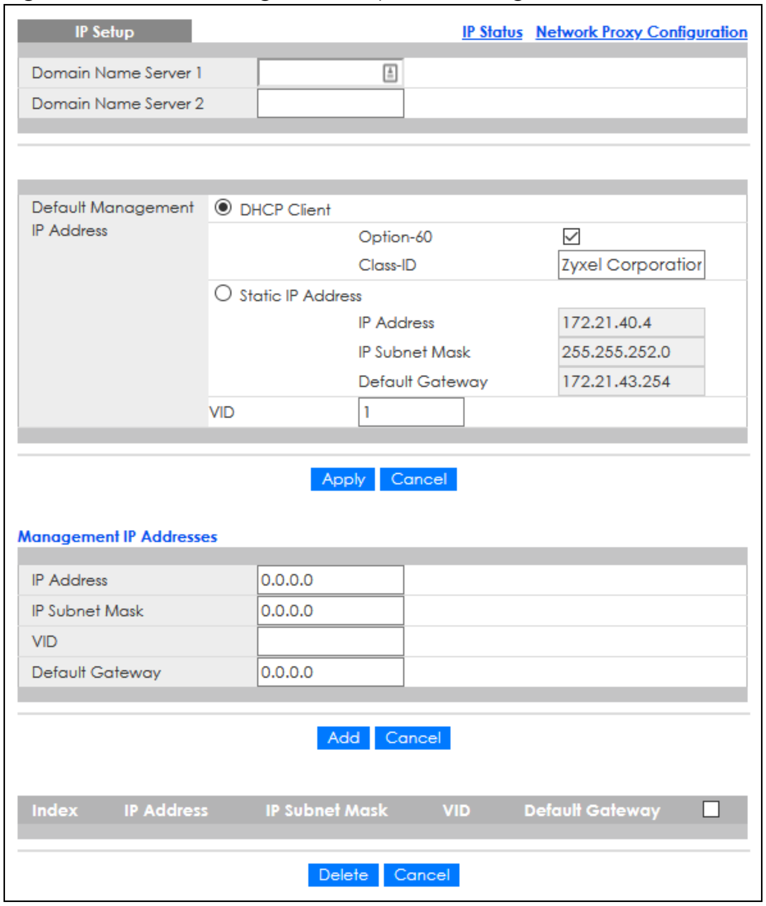
Table 29 Basic Setting > IP Setup > IP Status Details: DHCP

LABEL	DESCRIPTION
Type	This shows the IP address is dynamically assigned from a DHCP server (**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.

8.6.3 IP Configuration

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

Figure 86 Basic Setting > IP Setup > IP Configuration



The following table describes the labels in this screen.

Table 30 Basic Setting > IP Setup > IP Configuration

LABEL	DESCRIPTION
Domain Name Server 1/2	Enter a domain name server IPv4 address in order to be able to use a domain name instead of an IP address.
Default Management IP Address 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.
Option-60	DHCP Option 60 is used by the Switch for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Switch adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Select this and enter the device identity you want the Switch to add in the DHCP discovery frames that go to the DHCP server. This allows the Switch to identify itself to the DHCP server.
Class-ID	Type a string of up to 32 characters to identify this Switch to the DHCP server. For example, Zyxel-TW.
Static IP Address	Select this option if you do not 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, 172.21.40.x. This is the IP address of the Switch in an IP routing domain.

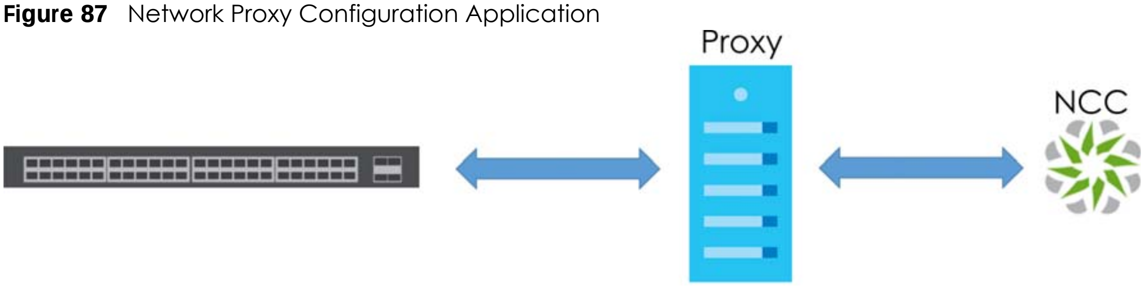
Table 30 Basic Setting > IP Setup > IP Configuration (continued)

LABEL	DESCRIPTION
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.252.0.
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 172.21.43.254.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
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.
Management IP Address Use these fields to set the settings for the 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.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.0.254.
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.
Default Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation.
	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.

8.6.4 Network Proxy Configuration

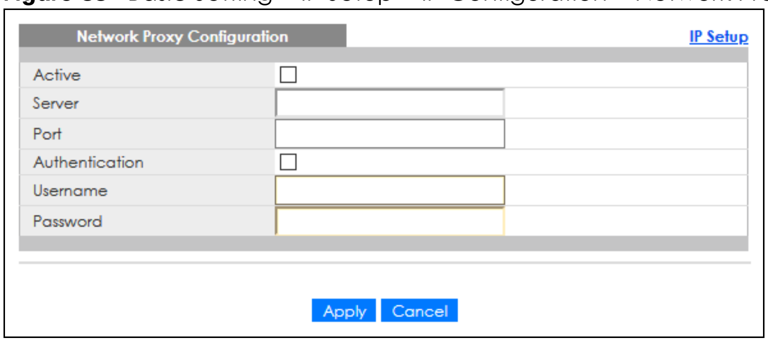
The proxy server of an organization may prohibit communication between the Switch and NCC (Nebula Control Center) (Section 8.11 on page 131). Use this screen to enable communication between the Switch and NCC through the proxy server.

Figure 87 Network Proxy Configuration Application



As of this writing, this setting only allows communication between the Switch and the NCC.

Figure 88 Basic Setting > IP Setup > IP Configuration > Network Proxy Configuration



The following table describes the labels in this screen.

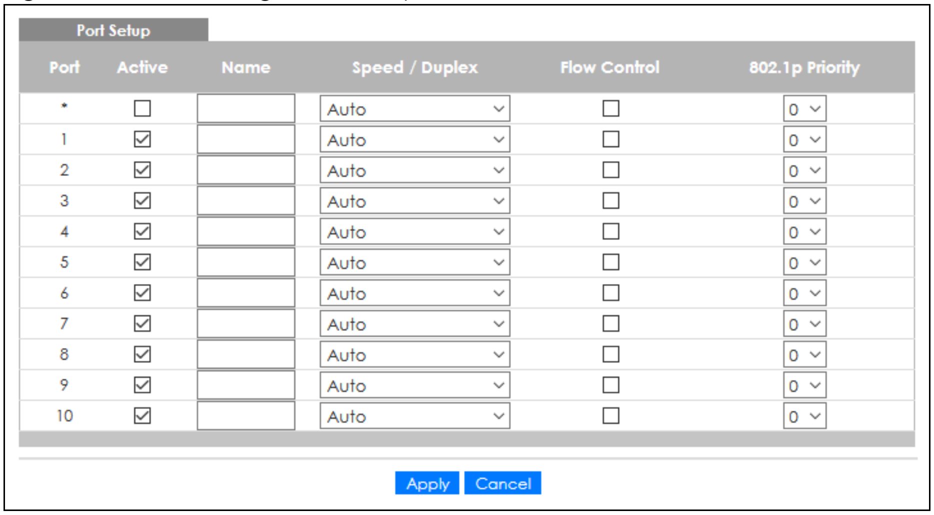
Table 31 Basic Setting > IP Setup > IP Configuration > Network Proxy Configuration

LABEL	DESCRIPTION
Active	Select this option to enable communication between the Switch and NCC through a proxy server.
Server	Enter the IP address (dotted decimal notation) or host name of the proxy server. When entering the host name, up to 128 alphanumeric characters are allowed for the **Server** including special characters inside the square quotes [~!@#$%^&*()_+{}|:”<>?-=[]\;’,./‘]
Port	Enter the port number of the proxy server (1 – 65535).
Authentication	Select this option to enable proxy server authentication using a **Username** and **Password**.
Username	Enter a login user name from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the **Username** including special characters inside the square quotes [~!@#$%^&*()_+{}|:”<>?-=[]\;’,./‘].
Password	Enter a login password from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the **Password** including special characters inside the square quotes [~!@#$%^&*()_+{}|:”<>?-=[]\;’,./‘].
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.

8.7 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 89 Basic Setting > Port Setup



The following table describes the labels in this screen.

Table 32 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some Web Configurator screens.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10-an** (10M/auto-negotiation), **10M/Half Duplex**, **10M/Full Duplex**, **100-an** (100M/auto-negotiation), **100M/Half Duplex**, **100M/Full Duplex** and **1G/Full Duplex** (Gigabit connections only). 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.

Table 32 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
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 IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x 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 26 on page 105 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.

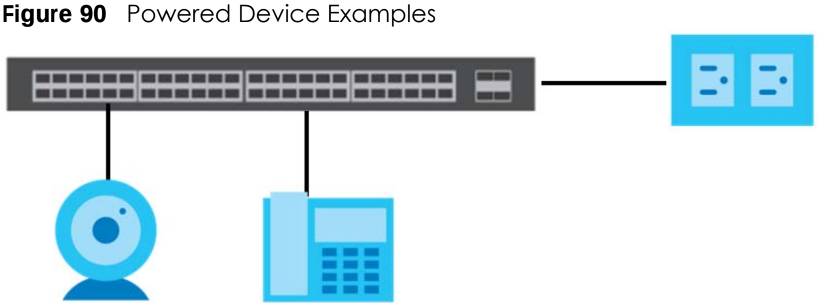
8.8 PoE Status

Note: The following screens are available for the PoE models only.

A powered device (PD) is a device such as an access point or a switch, that supports PoE (Power over Ethernet) so that it can receive power from another device through an Ethernet port.

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 90 Powered Device Examples

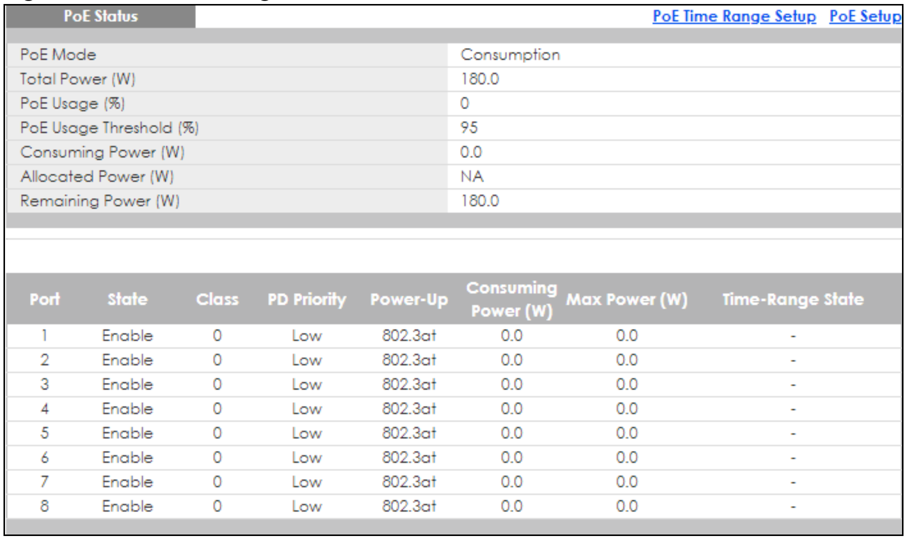


You can also set priorities so that the Switch is able to reserve and allocate power to certain PDs.

Note: The PoE (Power over Ethernet) 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 91 Basic Setting > PoE Status



PoE Status | PoE Time Range Setup | PoE Setup

PoE Mode	Consumption
Total Power (W)	180.0
PoE Usage (%)	0
PoE Usage Threshold (%)	95
Consuming Power (W)	0.0
Allocated Power (W)	NA
Remaining Power (W)	180.0

Port	State	Class	PD Priority	Power-Up	Consuming Power (W)	Max Power (W)	Time-Range State
1	Enable	0	Low	802.3at	0.0	0.0	-
2	Enable	0	Low	802.3at	0.0	0.0	-
3	Enable	0	Low	802.3at	0.0	0.0	-
4	Enable	0	Low	802.3at	0.0	0.0	-
5	Enable	0	Low	802.3at	0.0	0.0	-
6	Enable	0	Low	802.3at	0.0	0.0	-
7	Enable	0	Low	802.3at	0.0	0.0	-
8	Enable	0	Low	802.3at	0.0	0.0	-

The following table describes the labels in this screen.

Table 33 Basic Setting > PoE Status

LABEL	DESCRIPTION
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.
PoE Usage (%)	This field displays the amount of power currently being supplied to connected PoE devices (PDs) as a percentage of the total PoE power the Switch can supply. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in **Basic Setting** > **PoE Setup**.
PoE Usage Threshold (%)	This field displays the percentage of PoE usage. The Switch will generate a trap and/or a log when the usage exceeds the specified threshold.
Consuming Power (W)	This field displays the 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 (in classification mode) has reserved for PoE after negotiating with the connected PoE devices. It shows **NA** when the Switch is in consumption mode. **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	This is the port index number.
State	This field shows which ports can receive power from the Switch. You can set this in Section 8.8.2 on page 116. • **Disable** – The PD connected to this port cannot get power supply. • **Enable** – The PD connected to this port can receive power.

Table 33 Basic Setting > PoE Status (continued)

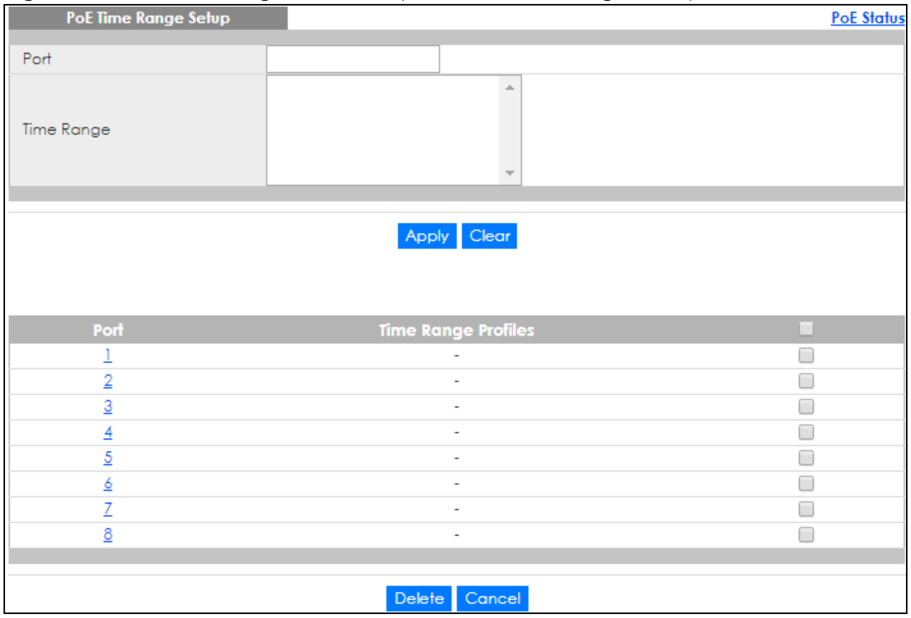
LABEL	DESCRIPTION
Class	This shows the power classification of the PD. Each PD has a specified maximum power that fall under one of the classes. The Class is a number from 0 to 4, where each value represents the range of power that the Switch provides to the PD. Each class corresponds to a default maximum power that can be extended in **Basic Setting** > **PoE Setup** > **PoE Setup** to the following values. • **Class 0** – default: 0.44 W to 15.4 W, can be extended to 17.8 W. • **Class 1** – default: 0.44 W to 4 W, can be extended to 5.8 W. • **Class 2** – default: 0.44 W to 7 W, can be extended to 9 W. • **Class 3** – default: 0.44 W to 15.4 W, can be extended to 17.8 W. • **Class 4** – default: 0.44 W to 30 W, can be extended to 32.8 W.
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	This field displays the PoE standard the Switch uses to provide power on this port.
Consuming Power (W)	This field displays the current amount of power consumed by the PD from the Switch on this port.
Max Power (W)	This field displays the maximum amount of power the PD could use from the Switch on this port.
Time-Range State	This field shows whether or not the port currently receives power from the Switch according to its schedule. • It shows "**In**" followed by the time range name if PoE is currently enabled on the port. • It shows "**Out**" if PoE is currently disabled on the port. • It shows **"–"** if no schedule is applied to the port. PoE is enabled by default.

8.8.1 PoE Time Range Setup

Use this screen to apply a schedule to the ports on the Switch. You must first configure a schedule in the **Advanced Application** > **Time Range** screen.

Click the **PoE Time Range Setup** link in the **Basic Setting** > **PoE Status** screen. The following screen opens.

Figure 92 Basic Setting > PoE Setup > PoE Time Range Setup



The following table describes the labels in this screen.

Table 34 Basic Setting > PoE Setup > PoE Time Range Setup

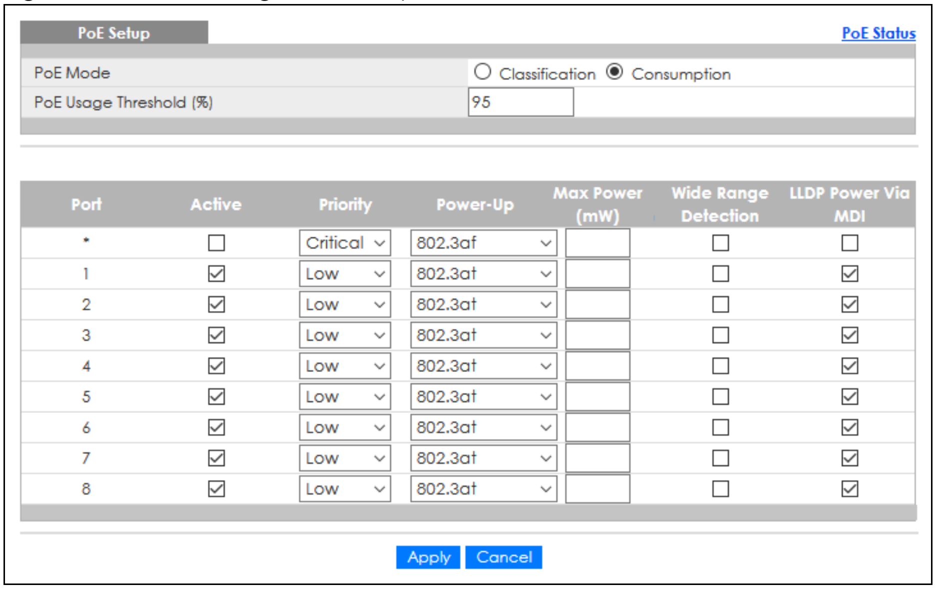
LABEL	DESCRIPTION
Port	Enter the number of the port to which you want to apply a schedule.
Time Range	This field displays the name of the schedule that you have created using the **Advanced Application** > **Time Range** screen. Select a pre-defined schedule to control when the Switch enables PoE to provide power on the port. To select more than one schedule, press [SHIFT] and select the choices at the same 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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Port	This field displays the index number of the port. Click a port number to change the schedule settings.
Time Range Profiles	This field displays the name of the schedule which is applied to the port. PoE is enabled at the specified time or date.
	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 and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

8.8.2 PoE Setup

Use this screen to set the PoE power management mode, priority levels, power-up mode and the maximum amount of power for the connected PDs.

Click the **PoE Setup** link in the **Basic Setting** > **PoE Status** screen. The following screen opens.

Figure 93 Basic Setting > PoE Setup



The following table describes the labels in this screen.

Table 35 Basic Setting > 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 maximum power for each PD according to the PD's power class and priority level. If the total power supply runs out, PDs with lower priority do not get power to function. In this mode, the maximum power is reserved based on what you configure in **Max Power** or the standard power limit for each class. • **Consumption** – Select this if you want the Switch to supply the actual power that the PD needs. The Switch also allocates power based on a port's **Max Power** and the PD's power class and priority level. The Switch puts a limit on the maximum amount of power the PD can request and use. In this mode, the default maximum power that can be delivered to the PD is 33 W (IEEE 802.3at Class 4) or 22 W (IEEE 802.3af Classes 0 to 3).
PoE Usage Threshold (%)	Enter a number ranging from 1 to 99 to set the threshold. The Switch will generate a trap and/or log when the actual PoE usage is higher than the specified threshold.
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	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.
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. Select **Critical** to give the highest PD priority on the port. 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.

Table 35 Basic Setting > PoE Setup (continued)

LABEL	DESCRIPTION
Power-Up	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. **Force-802.3at** – the Switch offers power of up to 33 W on the port without performing PoE hardware classification. Select this option if the connected PD does not comply with any PoE standard and requests power higher than a standard power limit.
Max Power (mW)	Specify the maximum amount of power the PD could use from the Switch on this port. If you leave this field blank, the Switch refers to the standard or default maximum power for each class. Note: The setting you enter here will NOT take effect when the power-up mode is set to **802.3bt**.
Wide Range Detection	Select this to let the Switch have a wider detection range for the PD. The Switch detects whether a connected device is a powered device or not before supplying power to the port. For the PD detection, the Switch applies a fixed voltage to the device and then receives returned current. If the returned current is within the IEEE 802.3AF/AT standard range, the device will be considered as a valid PD by the Switch. However, in real cases, environmental interferences might easily cause the returned current to be out of the standard range.
LLDP Power Via MDI	Select this to have the Switch negotiate PoE power with the PD connected to the port by transmitting LLDP Power Via MDI TLV frames. This helps the Switch allocate less power to the PD on this port. The connected PD must be able to request PoE power through LLDP. The Power Via MDI TLV allows PoE devices to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controllable • 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.

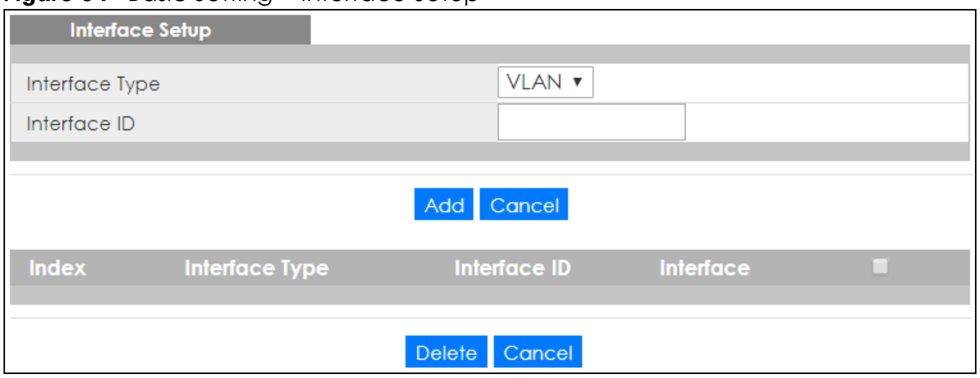
8.9 Interface Setup

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 94 Basic Setting > Interface Setup



The following table describes the labels in this screen.

Table 36 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. To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **Advanced Application** > **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.
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.

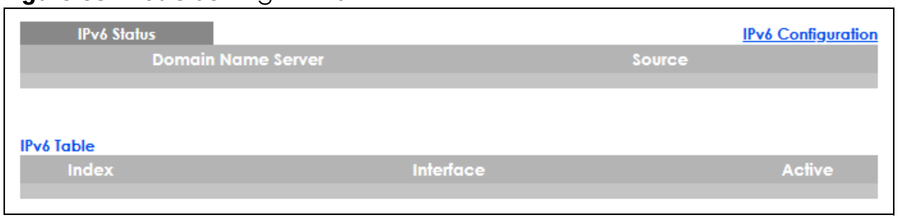
8.10 IPv6

Use this screen to view the IPv6 interface status and configure Switch's management IPv6 addresses.

8.10.1 IPv6 Status

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

Figure 95 Basic Setting > IPv6



The following table describes the labels in this screen.

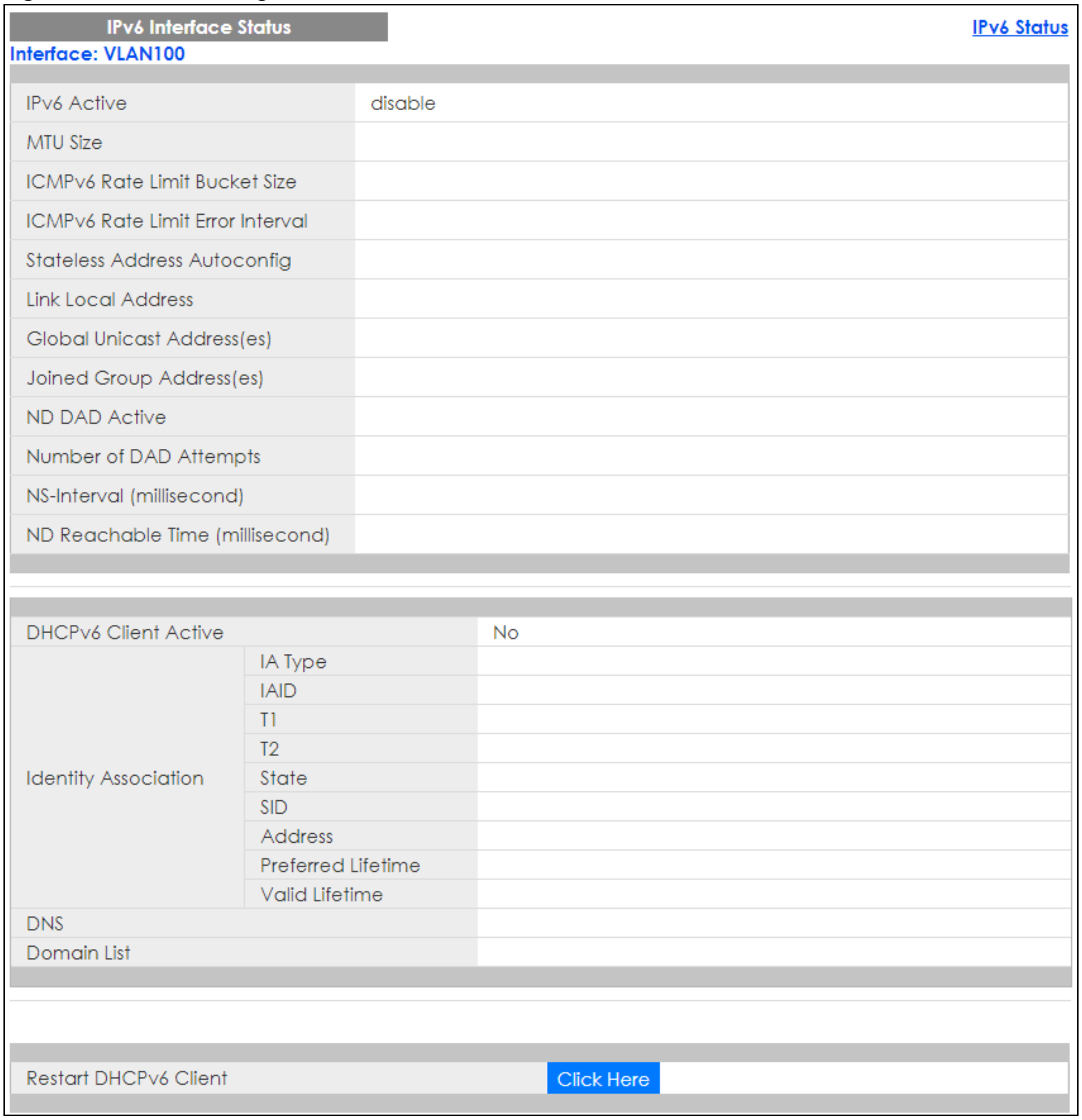
Table 37 Basic Setting > IPv6

LABEL	DESCRIPTION
IPv6 Status	
Domain Name Server	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 **DHCPv6**.
IPv6 Table	
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.

8.10.2 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 96 Basic Setting > IPv6 > IPv6 Interface Status



The following table describes the labels in this screen.

Table 38 Basic Setting > IPv6 > 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 auto-configuration.

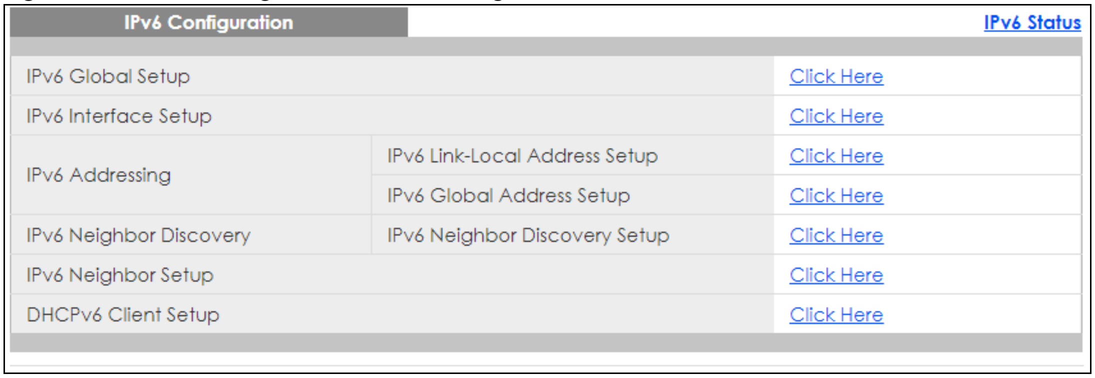
Table 38   Basic Setting > IPv6 > IPv6 Interface Status (continued)

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 does not 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.

8.10.3 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 97 Basic Setting > IPv6 > IPv6 Configuration



The following table describes the labels in this screen.

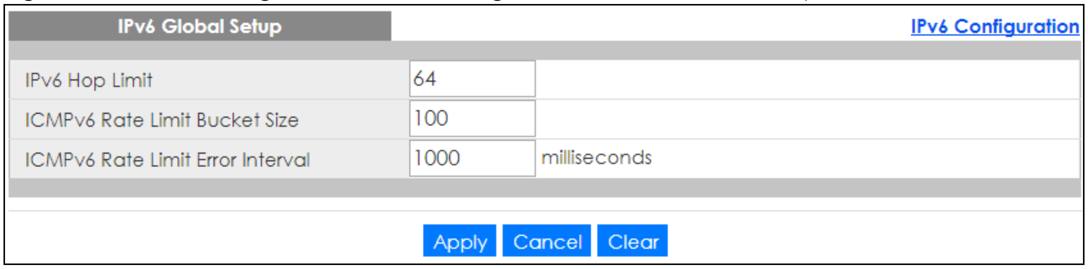
Table 39 Basic Setting > IPv6 > IPv6 Configuration

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 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 DHCPv6 client settings.

8.10.4 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 98 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup



The following table describes the labels in this screen.

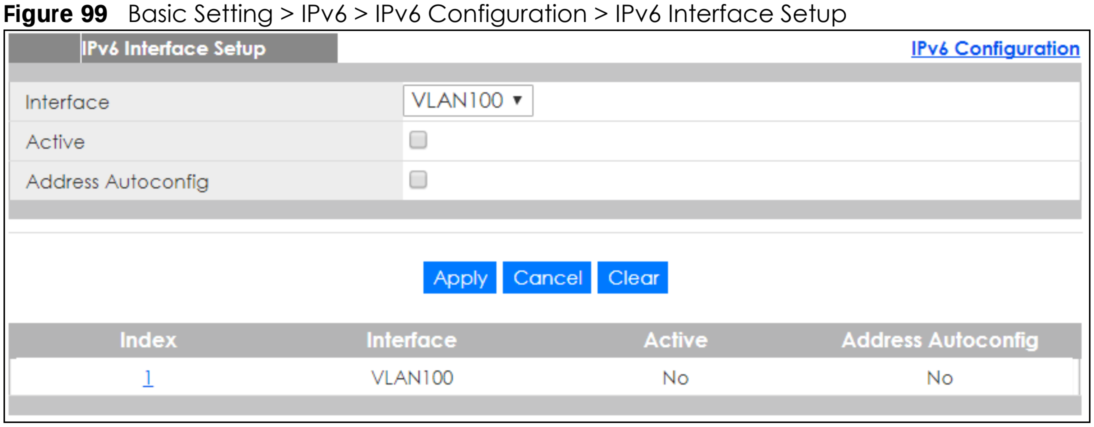
Table 40 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

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 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.

8.10.5 IPv6 Interface Setup

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

Figure 99 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup



The following table describes the labels in this screen.

Table 41   Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

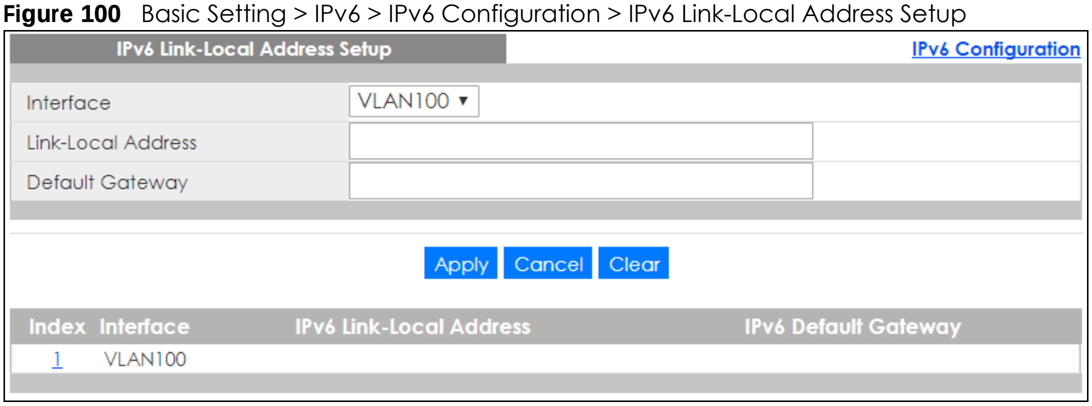
LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Active	Select this option to enable the interface.
Address Autoconfig	Select this option to allow the interface to automatically generate a link-local address via stateless auto-configuration.
Apply	Click **Apply** to save your 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 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 auto-configuration is enabled on the interface.

8.10.6 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 100   Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup



The following table describes the labels in this screen.

Table 42   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.
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.

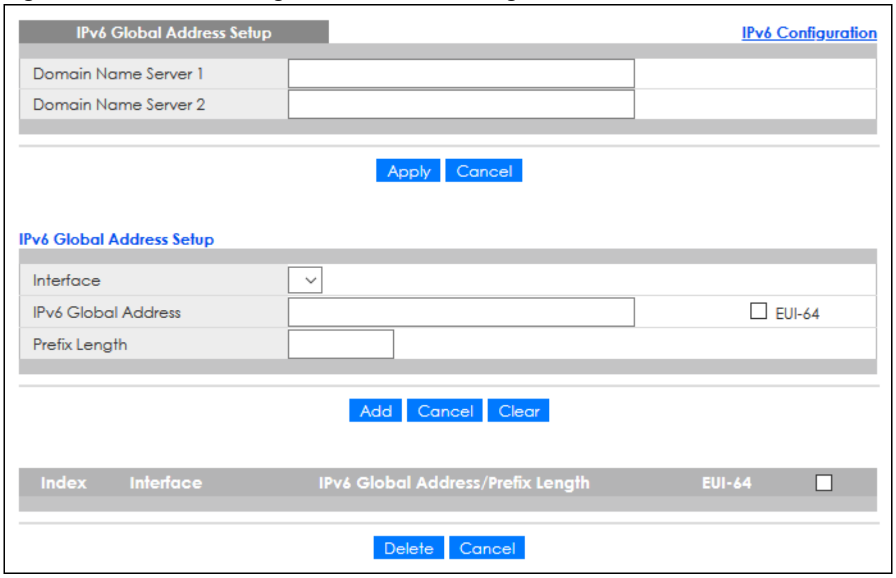
Table 42 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup (continued)

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.
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.

8.10.7 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 101 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup



The following table describes the labels in this screen.

Table 43 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

LABEL	DESCRIPTION
Domain Name Server 1/2	Enter a domain name server IPv6 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 non-volatile memory when you are done configuring.
Cancel	Click this to reset the **Domain Name Server** values in this screen to their last-saved values.
Interface	Select the IPv6 interface you want to configure.

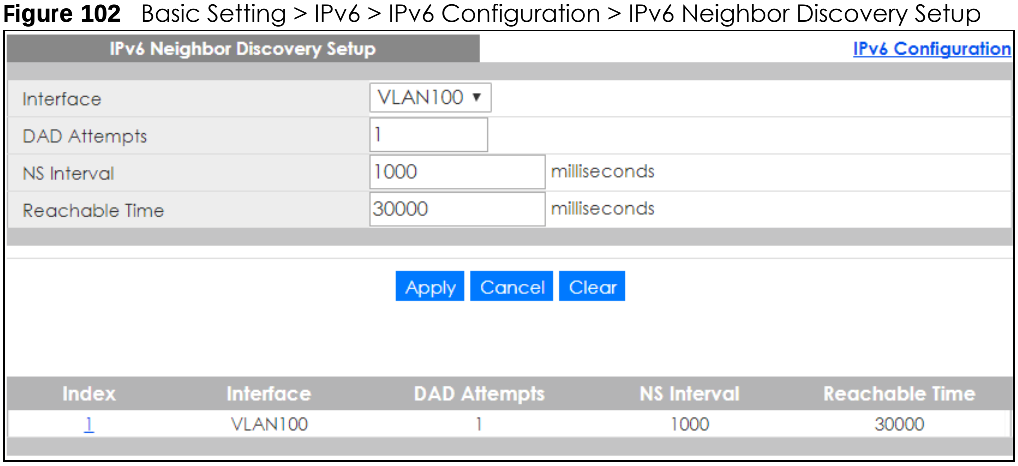
Table 43 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup (continued)

LABEL	DESCRIPTION
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 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.
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 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 entries that you want to remove and then click **Delete** to remove the selected entries from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

8.10.8 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 102 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup



The following table describes the labels in this screen.

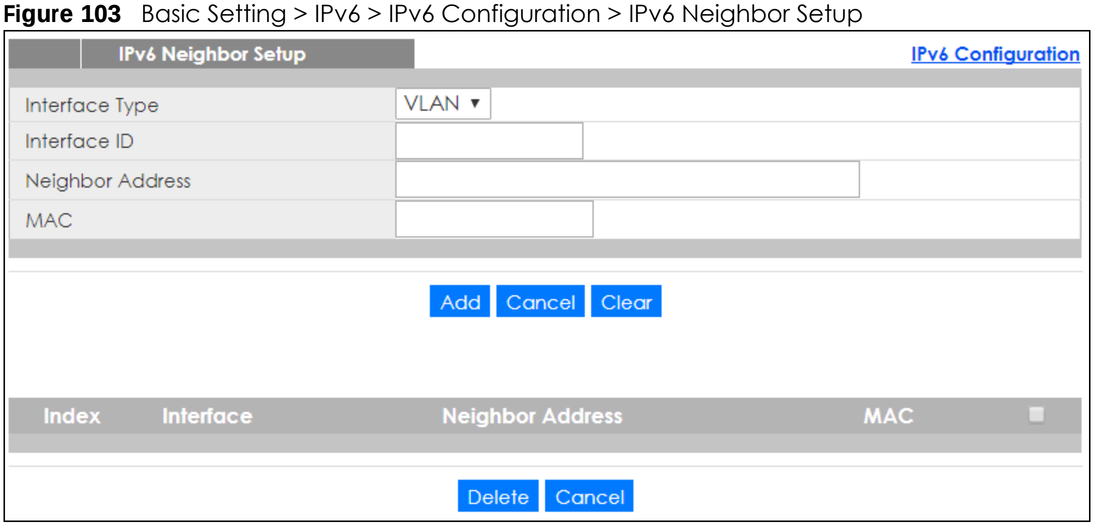
Table 44 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

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 auto-configuration. 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.
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 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.

8.10.9 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 103 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup



The following table describes the labels in this screen.

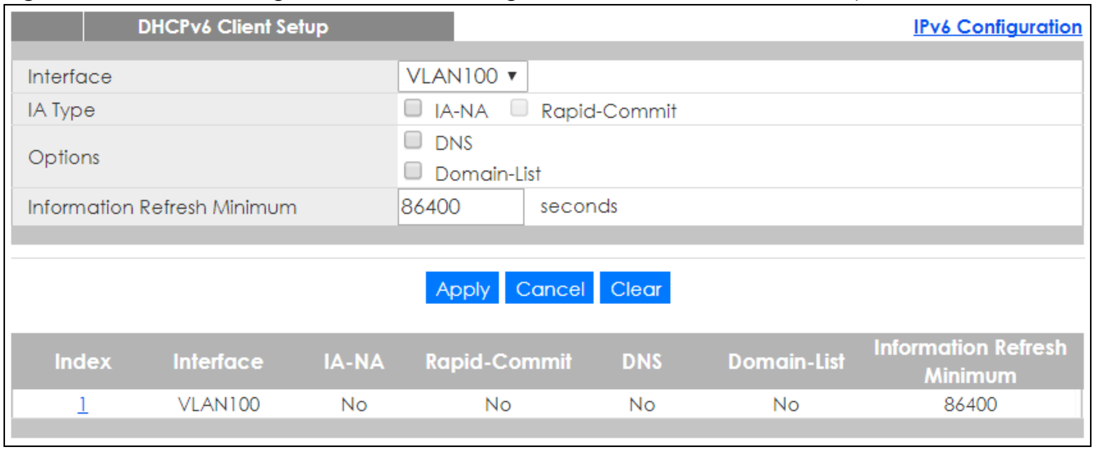
Table 45 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

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. A static IPv6 neighbor entry displays in the **Management** > **IPv6 Neighbor Table** screen only when the interface ID is also created in the **Basic Setup** > **Interface Setup** screen. To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **Advanced Application** > **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.
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 entries that you want to remove and then click **Delete** to remove the selected entries from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

8.10.10 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 **DHCPv6 Client Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 104 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup



The following table describes the labels in this screen.

Table 46 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.
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 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 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.

8.11 Cloud Management

The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula APs, Ethernet switches and security gateways.

The Switch is managed and provisioned automatically by the NCC (Nebula Control Center) when:

- It is connected to the Internet.
- The **Nebula Control Center Discovery** feature is enabled.
- It has been registered in the NCC.

This screen displays links to **Nebula Control Center Discovery** where you can have the Switch search for the NCC (Nebula Control Center) and to **Nebula Switch Registration** which has a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC.

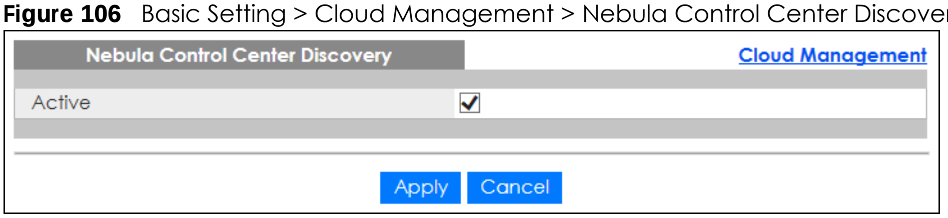
Click **Basic Setting** > **Cloud Management** in the navigation panel to display this screen.

Figure 105 Basic Setting > Cloud Management

8.11.1 Nebula Center Control Discovery

Click **Basic Setting** > **Cloud Management** > **Nebula Control Center Discovery** to display this screen.

Figure 106 Basic Setting > Cloud Management > Nebula Control Center Discovery



Select **Active** to turn on NCC discovery on the Switch. If the Switch has Internet access and has been registered in the NCC, it will go into cloud management mode.

In cloud management mode, then NCC will first check if the firmware on the Switch needs to be upgraded. If it does, the Switch will upgrade the firmware immediately. If the firmware does not need to be upgraded, but there is newer firmware available for the Switch, then it will be upgraded according to the firmware upgrade schedule for the Switch on the NCC. Below is the process for upgrading firmware:

1. Download firmware via the NCC.
2. Upgrade the firmware and reboot.

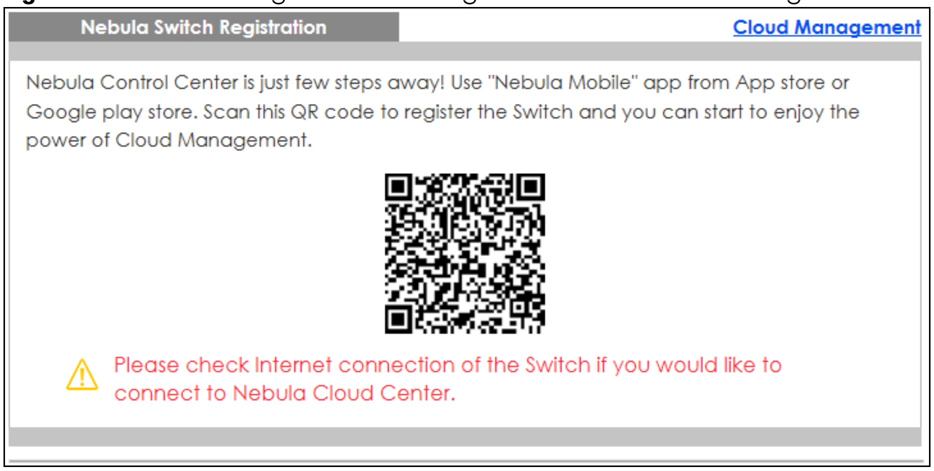
Note: While the Switch is rebooting, do NOT turn off the power.

Clear **Active** to turn off NCC discovery on the Switch. The Switch will NOT discover the NCC and remain in standalone mode.

8.11.2 Nebula Switch Registration

Click **Basic Setting** > **Cloud Management** > **Nebula Switch Registration** to display this screen.

Figure 107 Basic Setting > Cloud Management > Nebula Switch Registration



This screen has a QR code containing the Switch's serial number and MAC address for handy NCC registration of the Switch using the Nebula Mobile app. First, download the app from the Google Play store for Android devices or the App Store for iOS devices and create an organization and site.

CHAPTER 9
VLAN

9.1 Overview

This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen.

Note: If you have enabled CLV mode in the Command Line Interface (CLI) to configure the Switch's VLAN settings, further VLAN changes you make via the Web Configurator will not be saved and applied completely. You can still use the Web Configurator to view the VLAN status.

If you want to configure VLAN settings in both the Web Configurator and the CLI, just return to Zyxel configuration mode by turning off CLV mode. See the CLI Reference Guide for more information about CLV mode.

9.1.1 What You Can Do

- Use the **VLAN** screen (Section 9.3 on page 137) to view and search all static VLAN groups.
- Use the **VLAN Detail** screen (Section 9.3.1 on page 138) to view detailed port settings and status of the static VLAN group.
- Use the **Static VLAN Setup** screen (Section 9.5 on page 139) to configure a static VLAN for the Switch.
- Use the **VLAN Port Setup** screen (Section 9.6 on page 141) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **Subnet Based VLAN Setup** screen (Section 9.7 on page 142) to set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
- Use the **Protocol Based VLAN Setup** screen (Section 9.8 on page 145) to set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
- Use the **Voice VLAN Setup** screen (Section 9.9 on page 147) to set up VLANs that allow you to group voice traffic with defined priority and enable the Switch port to carry the voice traffic separately from data traffic to ensure the sound quality does NOT deteriorate.
- Use the **MAC Based VLAN Setup** screen (Section 9.10 on page 148) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. This eliminates the need to reconfigure the Switch when you change ports. The Switch will forward the packets based on the source MAC address you set up previously.
- Use the **Vendor ID Based VLAN Setup** screen (Section 9.11 on page 149) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. You can specify a mask for the MAC address to create a MAC address filter and enter a weight to set the VLAN rule's priority.
- Use the **Port-Based VLAN Setup** screen (Section 9.12 on page 151) to set up VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

9.1.2 What You Need to Know

Read this section to know more about VLAN and how to configure the screens.

9.2 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 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 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and 2 bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

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

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

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.

9.2.0.1 Automatic VLAN Registration

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

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.

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.

GVRP

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

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

Table 47 IEEE 802.1Q VLAN Terminology

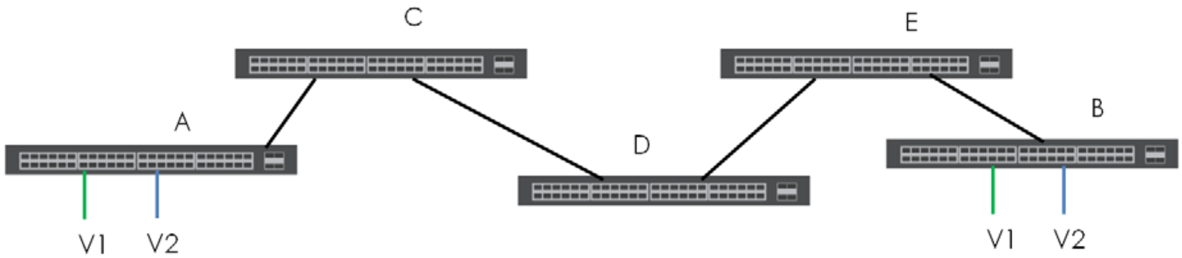
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration or de-registration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration 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 do not 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.

9.2.0.2 Port VLAN Trunking

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

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on ports 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 ports.

Figure 108 Port VLAN Trunking



9.2.0.3 VLAN Priority

At the time of writing, you can create Static VLANs, Voice VLANs, Vendor ID-based VLANs, Subnet Based VLANs, Protocol Based VLANs and MAC Based VLANs on the Switch when the VLAN type is set to 802.1Q. When a packet is received, the Switch processes the VLAN rules in sequence. The sequence (priority) of the VLANs is:

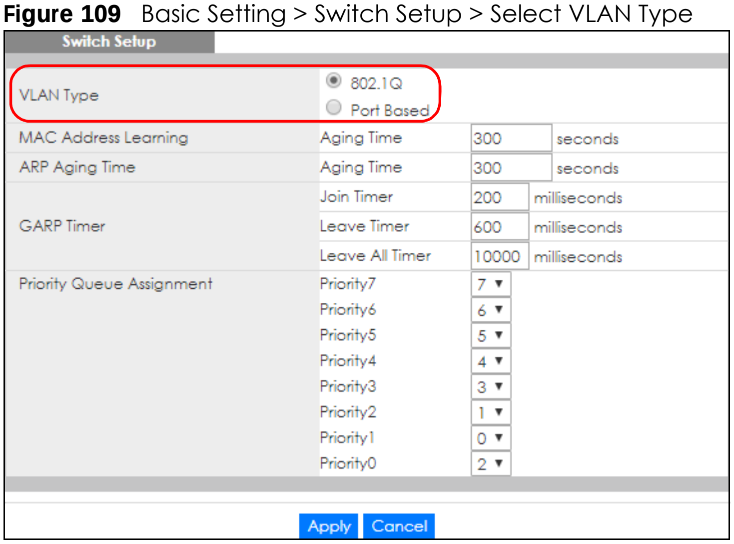
1. Vendor ID Based VLAN
2. Voice VLAN
3. Subnet Based VLAN
4. Protocol Based VLAN
5. MAC Based VLAN

If the packet matches a VLAN rule that has a higher priority, for example, an entry with weight 250 in the vendor ID to VLAN mapping table, the Switch assigns the corresponding VLAN ID to the packet and stops checking the subsequent VLAN rules.

9.2.0.4 Select the VLAN Type

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

Figure 109 Basic Setting > Switch Setup > Select VLAN Type



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

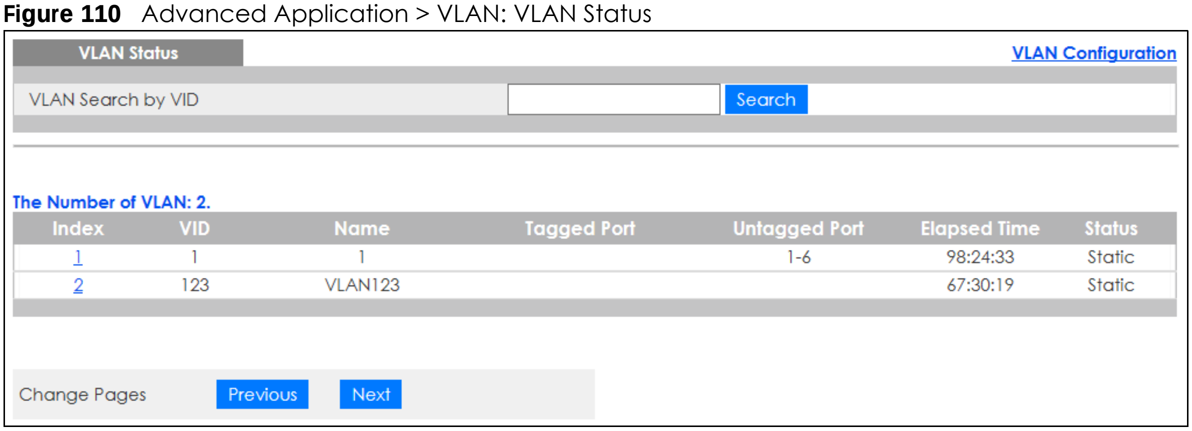
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

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

9.3 VLAN Status

Use this screen to view and search all static VLAN groups. Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 110 Advanced Application > VLAN: VLAN Status



The following table describes the labels in this screen.

Table 48 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID numbers (use a comma (,) to separate individual VLANs or a dash (–) to indicate a range of VLANs. For example, "3,4" or "3–9") and click **Search** to display only the specified VLANs 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 corresponding VLAN configuration screen.
Name	This fields shows the descriptive name of the VLAN.

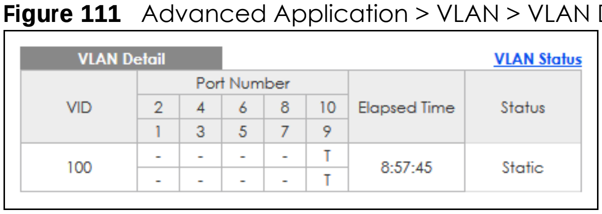
Table 48 Advanced Application > VLAN: VLAN Status (continued)

LABEL	DESCRIPTION
Tagged Port	This field shows the tagged ports that are participating in the VLAN.
Untagged Port	This field shows the untagged ports that are participating in the VLAN.
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. **Static**: added as a permanent entry.
Change Pages	Click **Previous** or **Next** to show the previous or next screen if all status information cannot be seen in one screen.

9.3.1 VLAN Details

Use this screen to view detailed port settings and status of the static VLAN group. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 111 Advanced Application > VLAN > VLAN Detail



The following table describes the labels in this screen.

Table 49 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
VID	This is the VLAN identification number that was configured in the corresponding VLAN configuration screen.
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**: added as a permanent entry **Voice**: manually added as a Voice VLAN **MVR**: added via multicast VLAN registration **MAC-based**: manually added as MAC-based VLAN

9.4 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 112 Advanced Application > VLAN > VLAN Configuration

The following table describes the labels in the above screen.

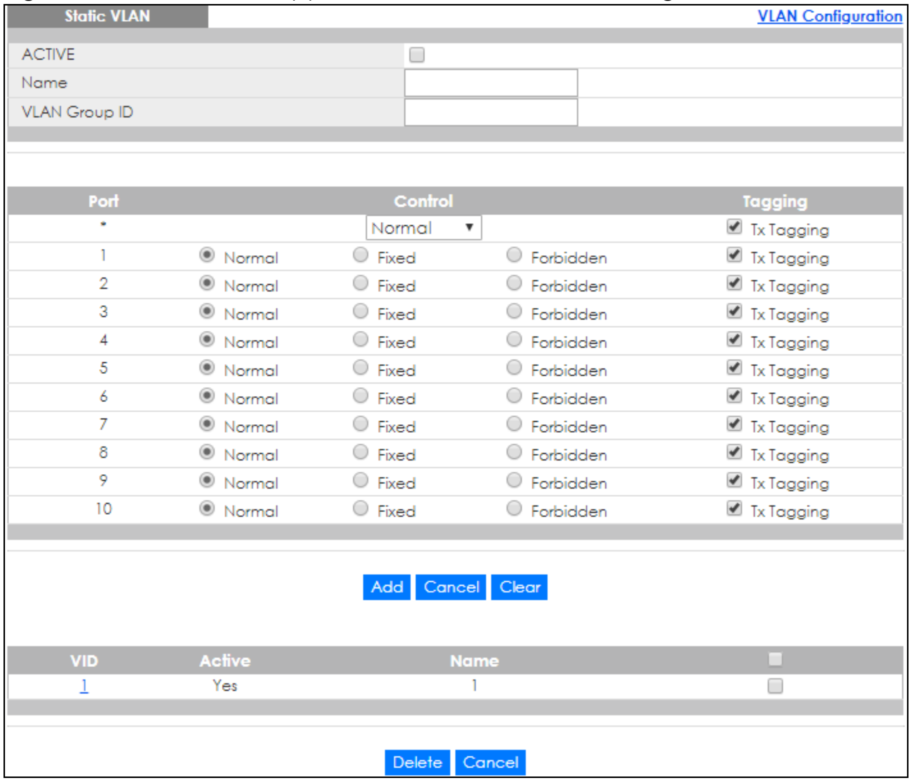
Table 50 Advanced Application > VLAN > VLAN Configuration

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.
Vendor ID Based VLAN Setup	Click **Click Here** to configure the Vendor ID Based VLAN for the Switch.

9.5 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 113 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup



The following table describes the related labels in this screen.

Table 51 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. Note: Do NOT add a VLAN ID that has been used in the **Voice VLAN Setup**.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select **Normal** for the port to dynamically join this VLAN group. 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 outgoing traffic to contain this VLAN tag. Otherwise, to ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

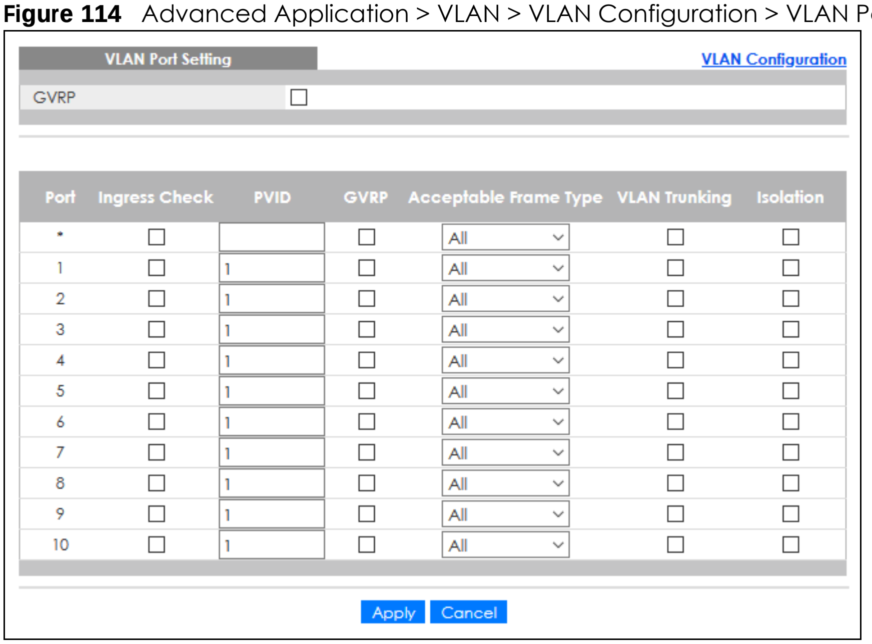
Table 51   Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup (continued)

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 start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this 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 from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

9.6 Configure VLAN Port Settings

Use this screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click the **VLAN Port Setup** link in the **VLAN Configuration** screen.

Figure 114   Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup



The following table describes the labels in this screen.

Table 52 Advanced Application > VLAN > VLAN Configuration> VLAN Port Setup

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected, the Switch discards incoming frames on a port 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 1and 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.
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.

9.7 Subnet Based VLANs

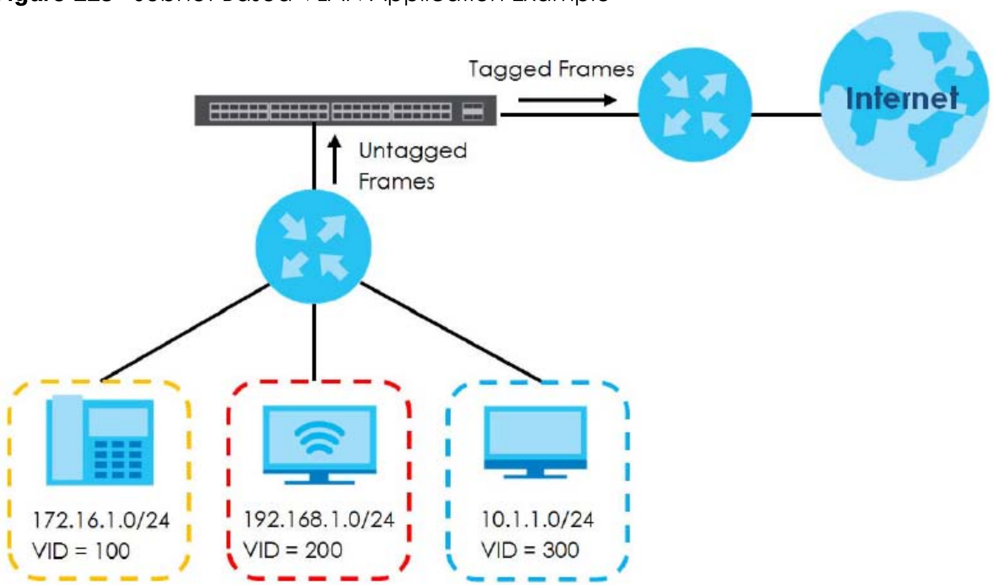
Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based 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 Services Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is video services receive the highest priority and data the lowest.

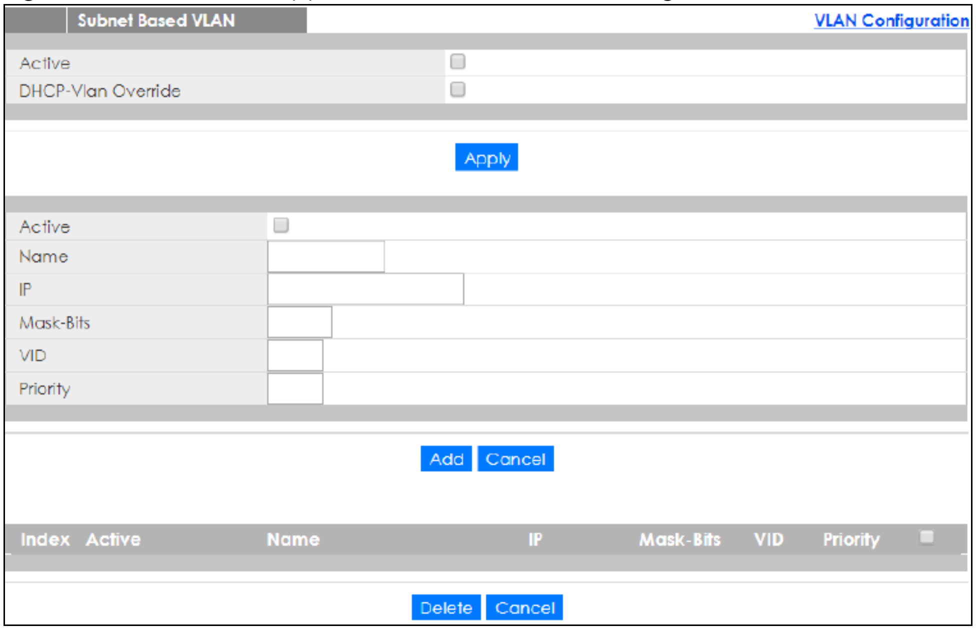
Figure 115 Subnet Based VLAN Application Example



9.7.1 Configuring Subnet Based VLAN

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

Figure 116 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup



The following table describes the labels in this screen.

Table 53 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this check box 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	Check this box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alpha numeric characters to identify this subnet based VLAN.
IP	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** screens.
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.

Table 53 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup (continued)

LABEL	DESCRIPTION
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
	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.

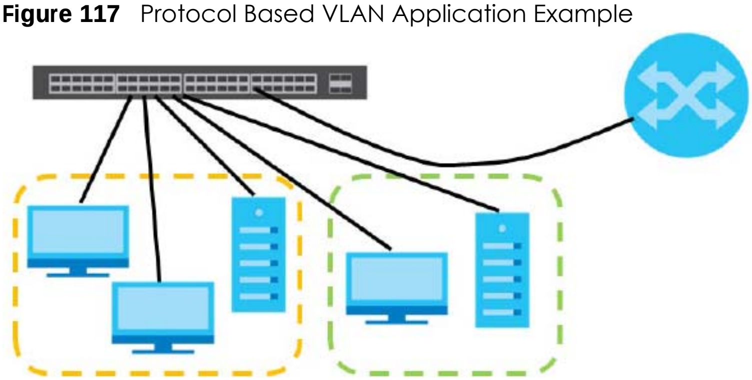
9.8 Protocol Based VLANs

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

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

For example, port 1, 2, 3 and 4 belong to static VLAN 100, and port 4, 5, 6, 7 belong to static VLAN 120. You configure a protocol based VLAN A with priority 3 for ARP traffic received on port 1, 2 and 3. You also have a protocol based VLAN B with priority 2 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic, when they go through the uplink port to a backbone switch C.

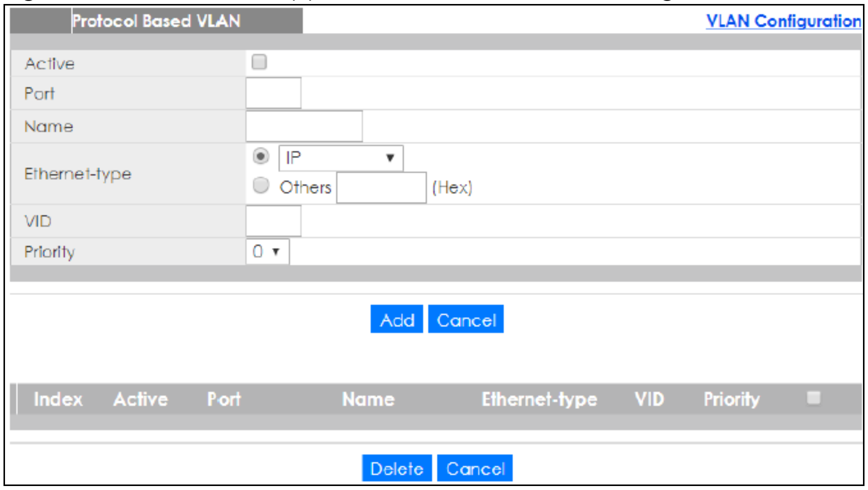
Figure 117 Protocol Based VLAN Application Example



9.8.1 Configuring Protocol Based VLAN

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

Figure 118 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup



The following table describes the labels in this screen.

Table 54 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this protocol based VLAN.
Port	Type a port to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN.
Name	Enter up to 32 alpha numeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select **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** screens.
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.
Name	This field shows the name the protocol based VLAN.
Ethernet-type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
	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 54   Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click **Cancel** to clear the check boxes.

9.9 Voice VLAN

Voice VLAN is a VLAN that is specifically allocated for voice traffic. It 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.

The Switch can determine whether a received packet is

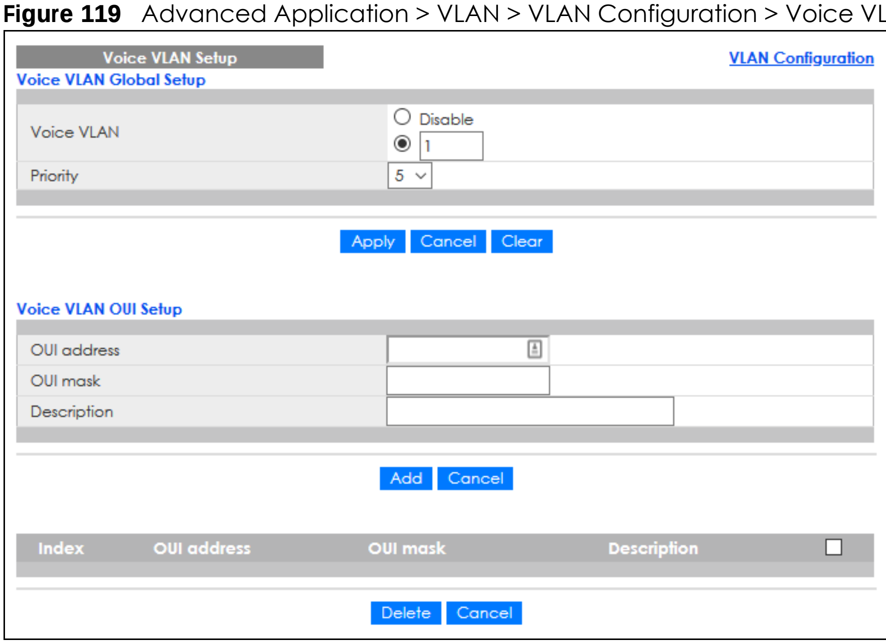
- an untagged voice packet when the incoming port is a fixed port for voice VLAN.
- a tagged voice packet when the incoming port and VLAN tag belongs to a voice VLAN.

It then checks the source packet's MAC address against an OUI list. If a match is found, the packet is considered as a voice packet.

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 119   Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup



The following table describes the fields in the above screen.

Table 55 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
Voice VLAN Global Setup	
Voice VLAN	Click the second radio button if you want to enable the Voice VLAN feature. Enter a VLAN ID number that is associated with the Voice VLAN. Click the **Disable** radio button if you do not want to enable the Voice VLAN feature.
Priority	Select the priority level of the voice traffic from 0 to 7. Default setting is 5. The higher the numeric value you assign, the higher the priority for this voice 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 section 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 3 byes is the manufacturer identifier, the last 3 bytes is a unique station ID.
OUI mask	Type the mask for the specified IP Phone manufacturer's OUI 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 bits of the matched traffic's MAC address, which can be of any hexadecimal characters. 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.
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 section 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.
	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.

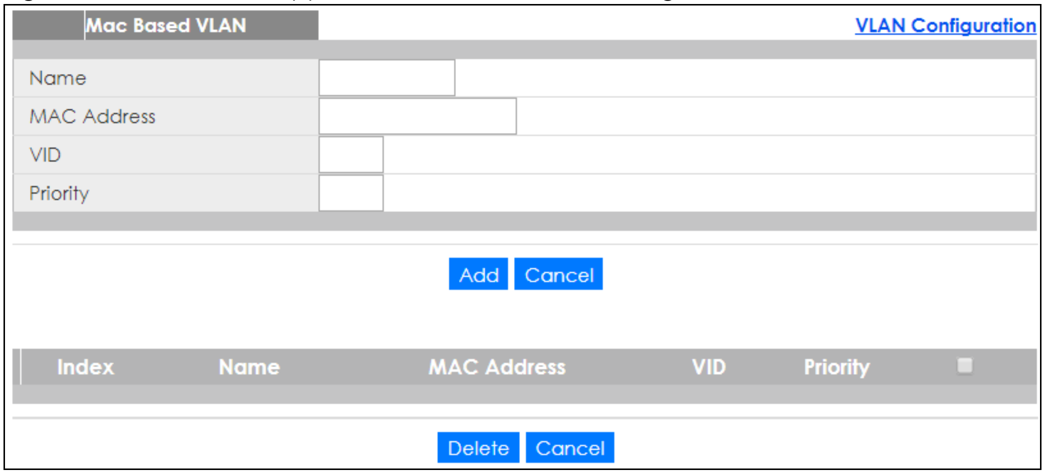
9.10 MAC Based VLAN

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 120 Advanced Application > VLAN > VLAN Configuration > MAC Based VLAN Setup



The following table describes the fields in the above screen.

Table 56 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 that is associated with the MAC-based VLAN entry.
Priority	Type a priority (0 to 7) that the Switch assigns to frames belonging to this VLAN. 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 which is assigned to frames belonging to this MAC-based VLAN entity.
	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.

9.11 Vendor ID Based VLAN

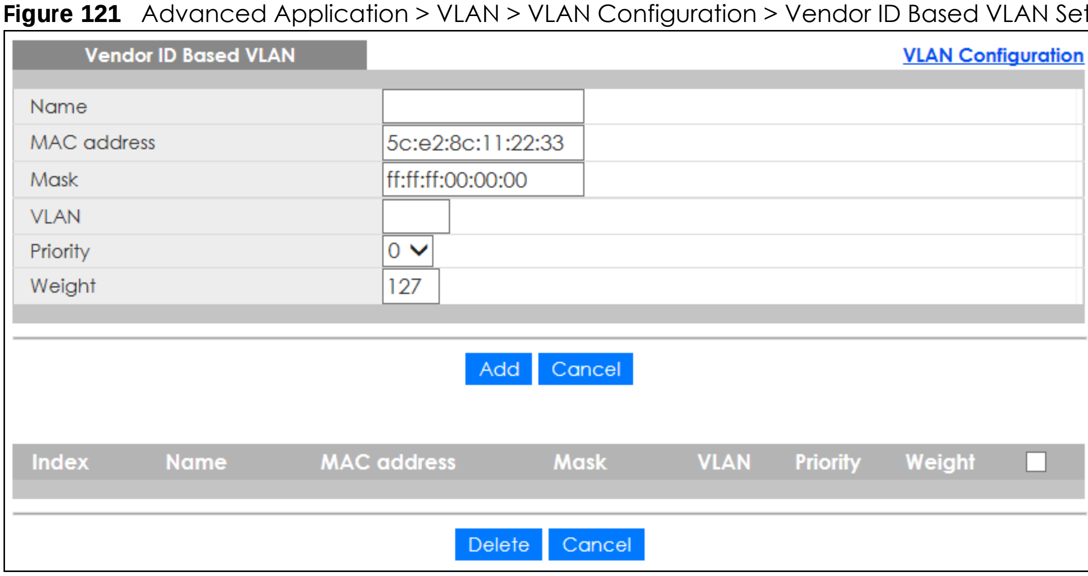
The Vendor ID based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. When untagged packets arrive at the switch, the source MAC address of the packet is looked up in a Vendor ID to VLAN mapping table. If an entry is found, 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 a 802.1p priority to the vendor ID based VLAN and define a vendor ID to VLAN mapping table by entering a specified source MAC address and mask in the vendor ID based VLAN setup screen. You can also delete a vendor ID based VLAN entry in the same screen.

For every vendor ID based VLAN rule you set, you can specify a weight number to define the rule's priority level. As rules are processed one after the other, stating a priority order will let you choose which rule has to be applied first and which second.

Click the **Vendor ID Based VLAN Setup** link in the **VLAN Configuration** screen to see the following screen.

Figure 121 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup



The following table describes the fields in the above screen.

Table 57 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup

LABEL	DESCRIPTION
Name	Type a name up to 32 alpha numeric characters for the vendor ID based VLAN entry.
MAC Address	Type a MAC address that is bind to the vendor ID-based VLAN entry. This is the source MAC address of the data packet that is looked up when untagged packets arrive at the Switch.
Mask	Type the mask for the specified source 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 bits of the matched traffic's MAC address, which can be of any hexadecimal characters. 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.
VLAN	Type an ID (from 1 to 4094) for the VLAN that is associated with the vendor ID based VLAN entry.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN. The higher the numeric value you assign, the higher the priority for this vendor ID based VLAN entry.

Table 57 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup

LABEL	DESCRIPTION
Weight	Enter a number between 0 and 255 to specify the rule's weight. This is to decide the priority in which the rule is applied. The higher the number, the higher the rule's priority.
Add	Click **Add** to save the new vendor ID based VLAN entry.
Cancel	Click **Cancel** to clear the fields in the vendor ID based VLAN entry.
Index	This field displays the index number of the vendor ID based VLAN entry.
Name	This field displays the name of the vendor ID based VLAN entry.
MAC Address	This field displays the source MAC address that is bind to the vendor ID based VLAN entry.
Mask	This field displays the mask for the source MAC address that is bind to the vendor ID based VLAN entry.
VLAN	This field displays the VLAN ID of the vendor ID based VLAN entry.
Priority	This field displays the priority level which is assigned to frames belonging to this vendor ID based VLAN.
Weight	This field displays the weight of the vendor ID 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.

9.12 Port-Based VLAN Setup

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

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

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

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

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

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

9.12.1 Configure a Port-Based VLAN

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

Figure 122 Advanced Application > VLAN: Port Based VLAN Setup (All Connected)

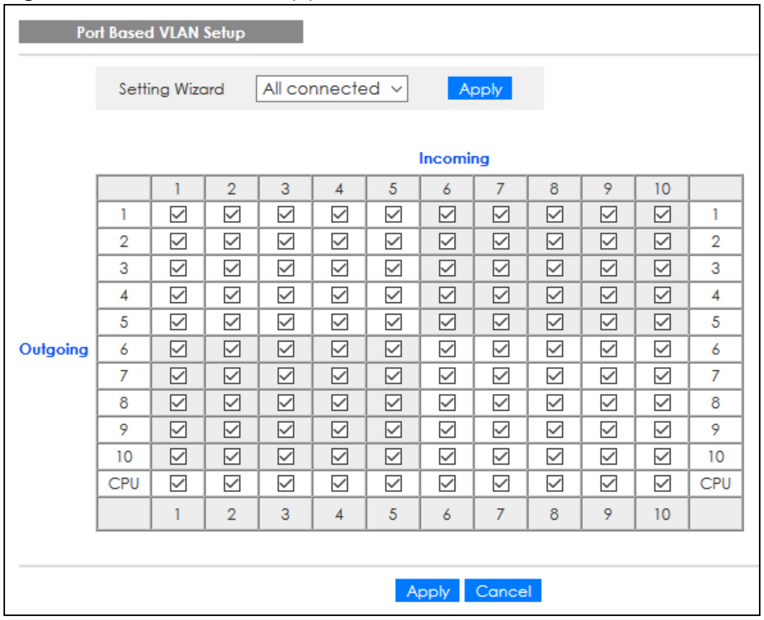
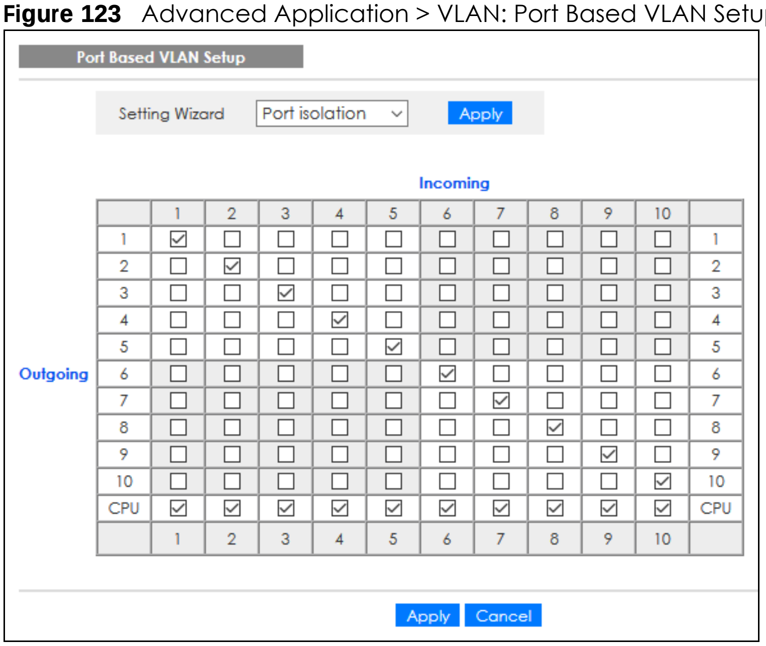


Figure 123 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 58   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 or 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.

CHAPTER 10
Static MAC Forwarding

10.1 Overview

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

Use these screens to configure static MAC address forwarding.

10.1.1 What You Can Do

Use the **Static MAC Forwarding** screen (Section 10.2 on page 154) to assign static MAC addresses for a port.

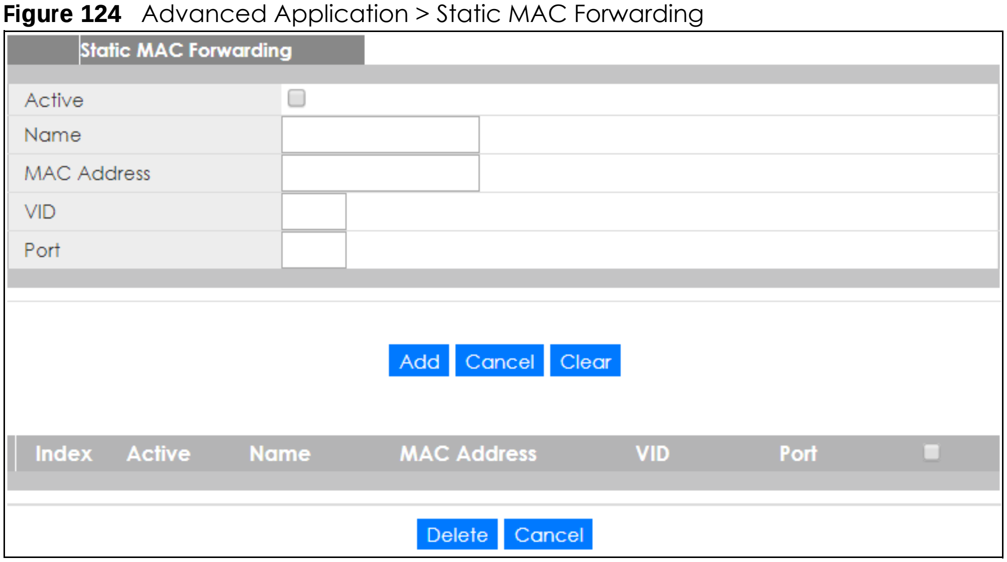
10.2 Configure Static MAC Forwarding

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

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch. See Chapter 19 on page 205 for more information on port security.

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

Figure 124 Advanced Application > Static MAC Forwarding



The following table describes the labels in this screen.

Table 59 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	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
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 begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**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.
	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.

CHAPTER 11 Static Multicast Forwarding

11.1 Overview

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

Use these screens to configure static multicast address forwarding.

11.1.1 What You Can Do

Use the **Static Multicast Forwarding** screen (Section 11.2 on page 157) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific ports.

11.1.2 What You Need To Know

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. Figure 125 on page 156 shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to ports within a VLAN group. Figure 126 on page 157 shows frames being forwarded to devices connected to port 3. Figure 127 on page 157 shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 125 No Static Multicast Forwarding

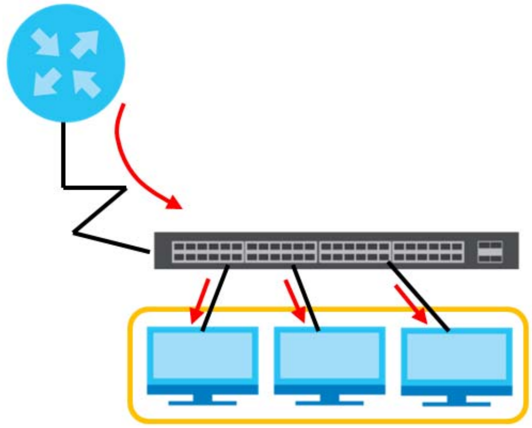


Figure 126 Static Multicast Forwarding to A Single Port

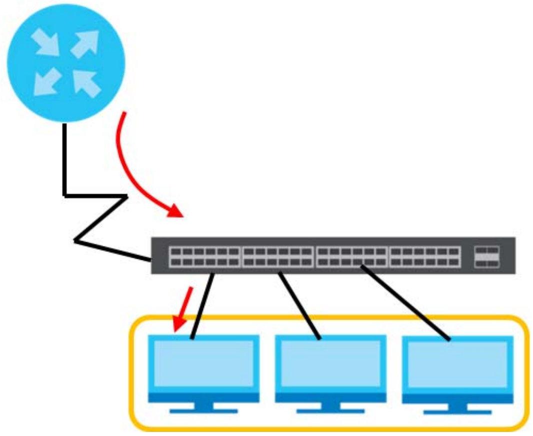
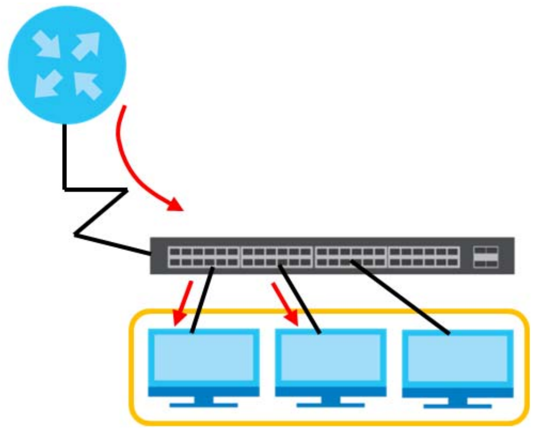


Figure 127 Static Multicast Forwarding to Multiple Ports

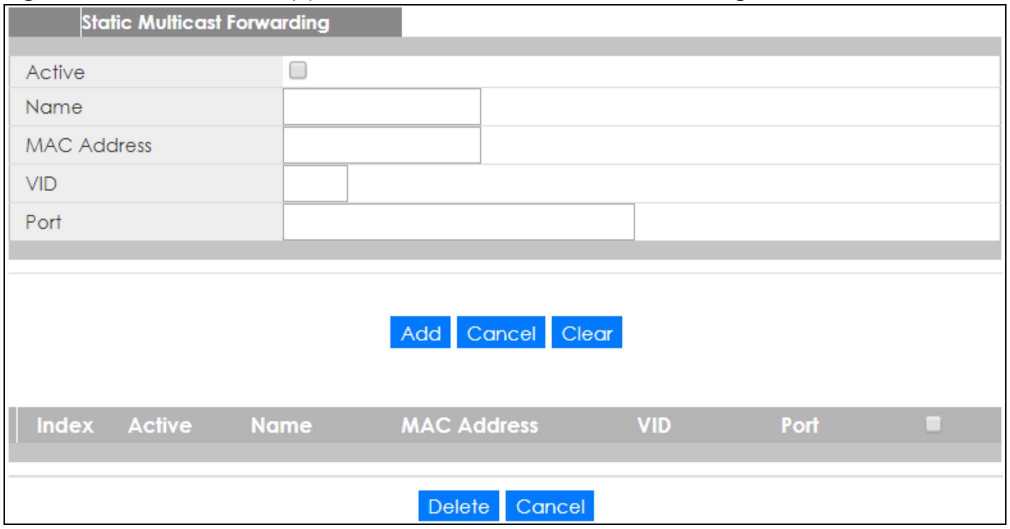


11.2 Configure Static Multicast Forwarding

Use this screen to configure rules to forward specific multicast frames, such as streaming or control frames, to specific ports.

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

Figure 128 Advanced Application > Static Multicast Forwarding



The following table describes the labels in this screen.

Table 60 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 ports within a VLAN group. Enter the ID that identifies the VLAN group here. If you do NOT have a specific target VLAN, enter 1.
Port	Enter the ports where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (–). For example, enter “3–5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Add	Click 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 begin configuring this screen afresh.
Index	Click an index number to modify a static multicast MAC address rule for ports.
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 ports within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.

Table 60 Advanced Application > Static Multicast Forwarding (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	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the check boxes.

CHAPTER 12 Filtering

12.1 Filtering Overview

This chapter discusses MAC address port filtering.

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

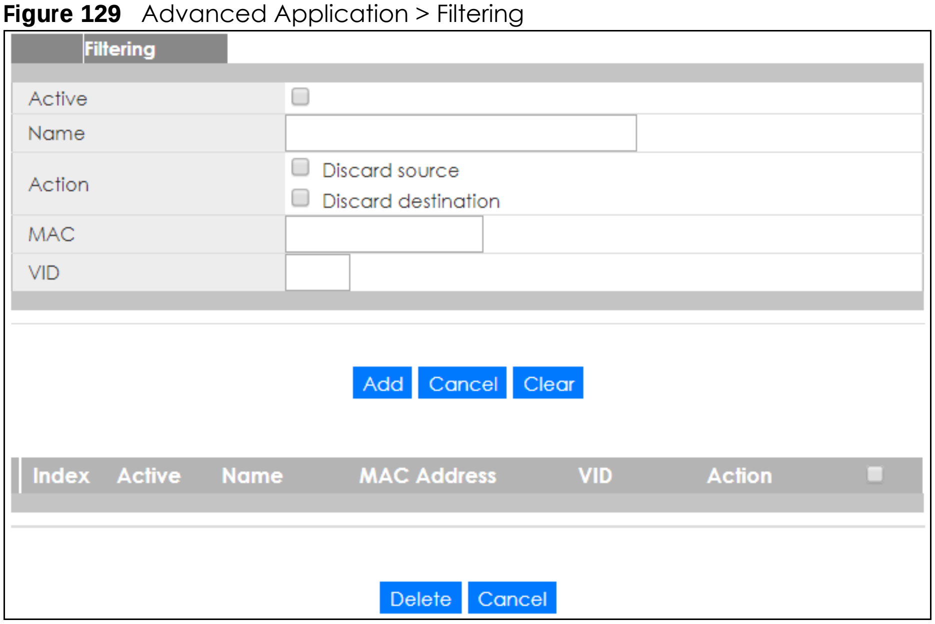
12.1.1 What You Can Do

Use the **Filtering** screen (Section 12.2 on page 160) to create rules for traffic going through the Switch.

12.2 Configure a Filtering Rule

Use this screen to create rules for traffic going through the Switch. Click **Advanced Application** > **Filtering** in the navigation panel to display the screen as shown next.

Figure 129 Advanced Application > Filtering



The following table describes the related labels in this screen.

Table 61 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 de-selecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.
Action	Select **Discard source** to drop the 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 the 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 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 reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **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 purpose only.
MAC Address	This field displays the source or 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 rules that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

CHAPTER 13 Spanning Tree Protocol

13.1 Spanning Tree Protocol Overview

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.

13.1.1 What You Can Do

- Use the **Spanning Tree Protocol Status** screen (Section 13.2 on page 165) to view the STP status in the different STP modes (RSTP, MRSTP or MSTP) you can configure on the Switch.
- Use the **Spanning Tree Configuration** screen (Section 13.6.1 on page 174) to activate one of the STP modes on the Switch.
- Use the **Rapid Spanning Tree Protocol Status** screen (Section 13.4 on page 166) to view the RSTP status.
- Use the **Rapid Spanning Tree Protocol** screen (Section 13.5 on page 168) to configure RSTP settings.
- Use the **Multiple Spanning Tree Protocol** screen (Section 13.6 on page 169) to configure MSTP.
- Use the **Multiple Spanning Tree Protocol Status** screen (Section 13.7 on page 174) to view the MSTP status.
- Use the **Multiple Rapid Spanning Tree Protocol** screen (Section 13.8 on page 177) to configure MRSTP.
- Use the **Multiple Rapid Spanning Tree Protocol Status** screen (Section 13.9 on page 179) to view the MRSTP status.

13.1.2 What You Need to Know

Read on for concepts on STP that can help you configure the screens in this chapter.

(Rapid) Spanning Tree Protocol

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

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

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

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 62 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4 Mbps	250	100 to 1000	1 to 65535
Path Cost	10 Mbps	100	50 to 600	1 to 65535
Path Cost	16 Mbps	62	40 to 400	1 to 65535
Path Cost	100 Mbps	19	10 to 60	1 to 65535
Path Cost	1 Gbps	4	3 to 10	1 to 65535
Path Cost	10 Gbps	2	1 to 5	1 to 65535

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

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

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.

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 63 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.

Multiple STP

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

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

Multiple RSTP

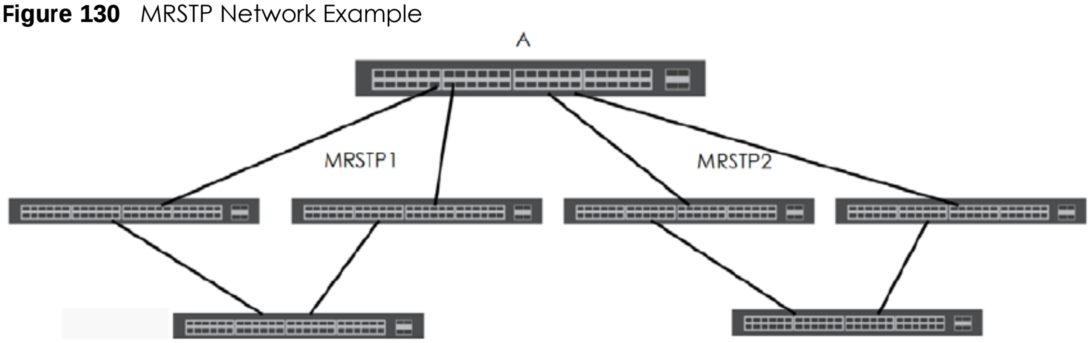
MRSTP (Multiple RSTP) is Zyxel's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign ports to each tree. Each spanning tree operates independently with its own bridge information.

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

To set up MRSTP, activate MRSTP on the Switch and specify which ports belong to which spanning tree.

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

Figure 130 MRSTP Network Example



Multiple STP

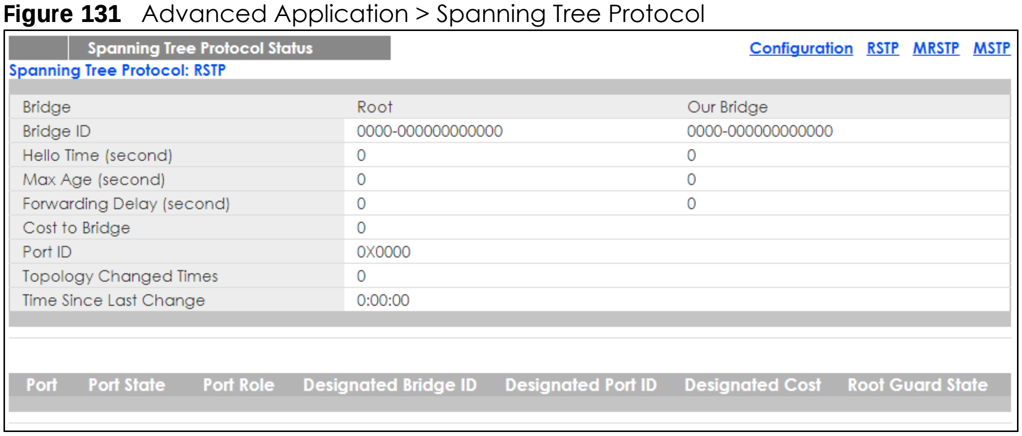
Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

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

13.2 Spanning Tree Protocol Status

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

Figure 131 Advanced Application > Spanning Tree Protocol

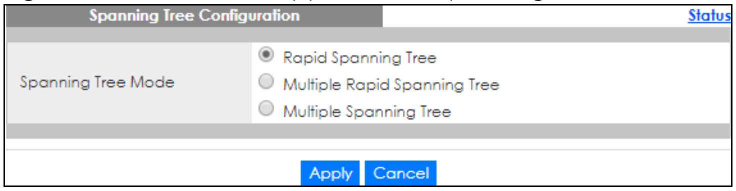


This screen differs depending on which STP mode (RSTP or MSTP) you configure on the Switch. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the Switch.

13.3 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 132 Advanced Application > Spanning Tree Protocol > Configuration



The following table describes the labels in this screen.

Table 64 Advanced Application > Spanning Tree Protocol > Configuration

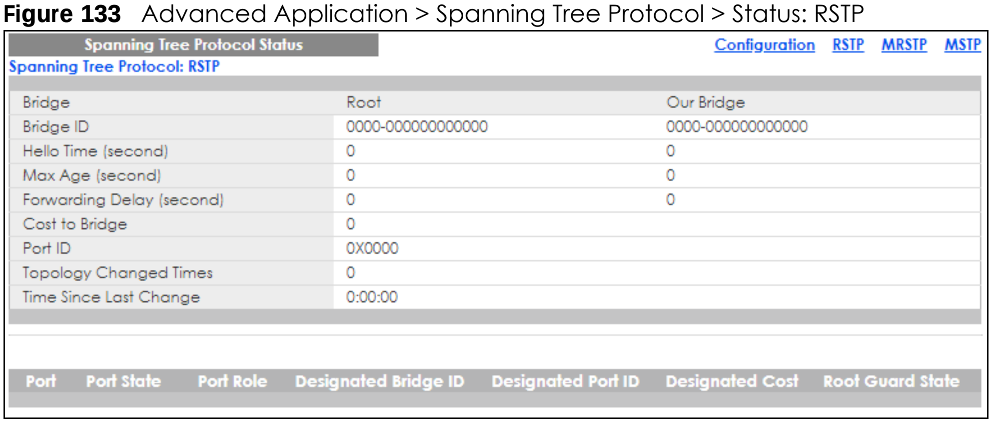
LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree**, **Multiple Rapid Spanning Tree** or **Multiple Spanning Tree**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is 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.

13.4 Rapid Spanning Tree Protocol Status

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 13.1 on page 162 for more information on RSTP.

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

Figure 133 Advanced Application > Spanning Tree Protocol > Status: RSTP



The following table describes the labels in this screen.

Table 65 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.

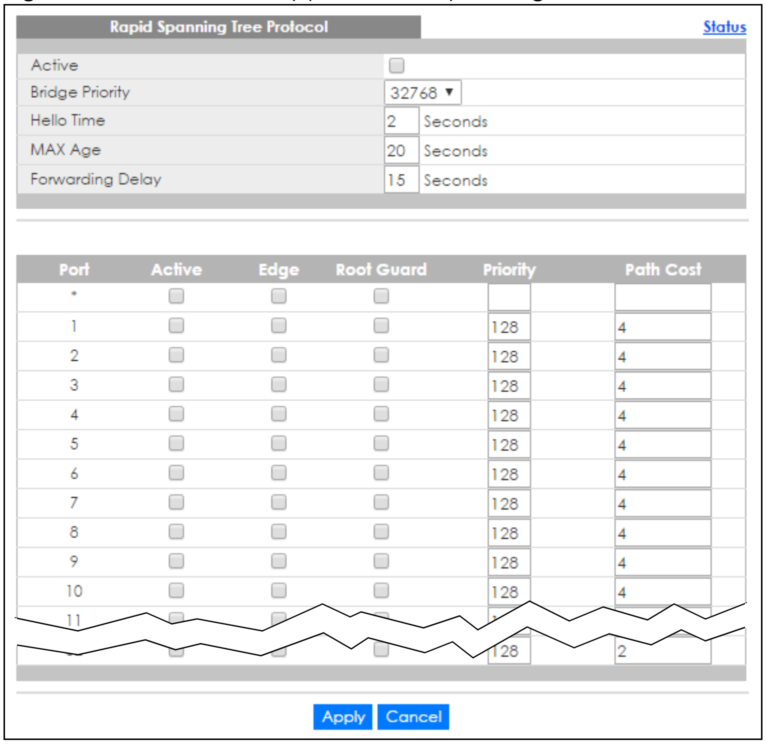
Table 65 Advanced Application > Spanning Tree Protocol > Status: RSTP (continued)

LABEL	DESCRIPTION
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) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). 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 or 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 or 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 segment to which this port is connected.
Root Guard State	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 unblocks and allows the port to forward frames again.

13.5 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 13.1 on page 162 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 134 Advanced Application > Spanning Tree Protocol > RSTP



The following table describes the labels in this screen.

Table 66 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen.
Active	Select this check box to activate RSTP. Clear this check box 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.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

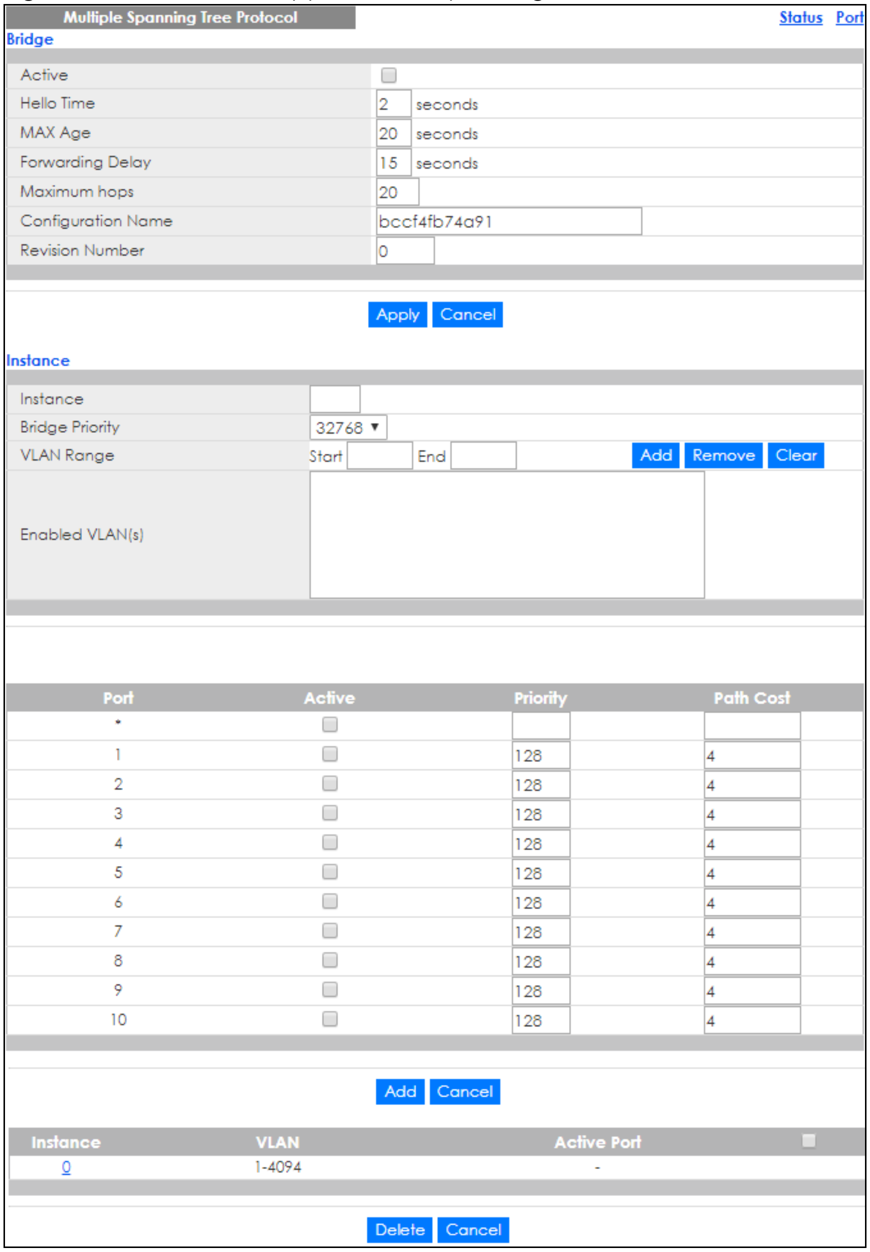
Table 66 Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every Switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
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	Select this check box to enable root guard on this port in order to prevent the switches 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.
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.

13.6 Configure Multiple Spanning Tree Protocol

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

Figure 135 Advanced Application > Spanning Tree Protocol > MSTP



The following table describes the labels in this screen.

Table 67 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MSTP Status** screen.
Port	Click **Port** to display the **MSTP Port** screen.
Active	Select this check box to activate MSTP on the Switch. Clear this check box 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 67 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 – 15.
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 VLANs to be mapped to the MST instance. • **Remove** – to remove this range of VLANs from being mapped to the MST instance. • **Clear** – to remove all VLANs from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLANs are mapped to this MST instance.
Port	This field displays 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 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.

Table 67 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
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.
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. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rules that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

The following table describes the labels in this screen.

Table 68 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MSTP Status** screen.
Port	Click **Port** to display the **MSTP Port** screen.
Active	Select this to activate MSTP on the Switch. Clear this 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.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: 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.

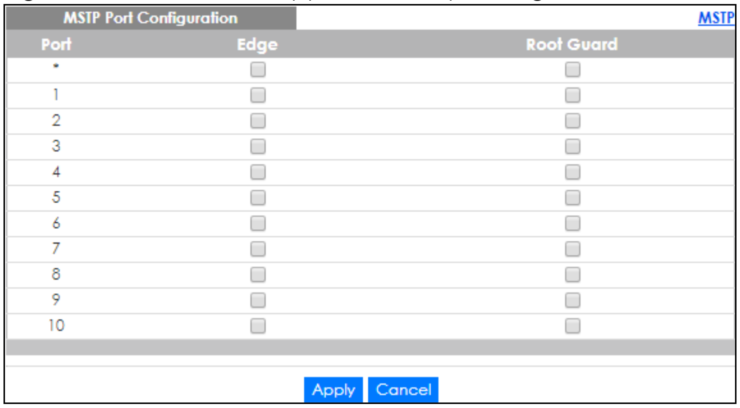
Table 68 Advanced Application > Spanning Tree Protocol > MSTP (continued)

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.
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. Note: The Switch supports instance numbers 0 – 15.
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 VLANs to be mapped to the MST instance. • **Remove** – to remove this range of VLANs from being mapped to the MST instance. • **Clear** – to remove all VLANs from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLANs are mapped to this MST instance.
Port	This field displays 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 add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
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. Click this number to modify its settings.
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. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rules that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

13.6.1 Multiple Spanning Tree Protocol Port Configuration

Click **Advanced Application** > **Spanning Tree Protocol** > **MSTP** > **Port** in the navigation panel to display the status screen as shown next.

Figure 136 Advanced Application > Spanning Tree Protocol > MSTP > Port



The following table describes the labels in this screen.

Table 69 Advanced Application > Spanning Tree Protocol > MSTP > Port

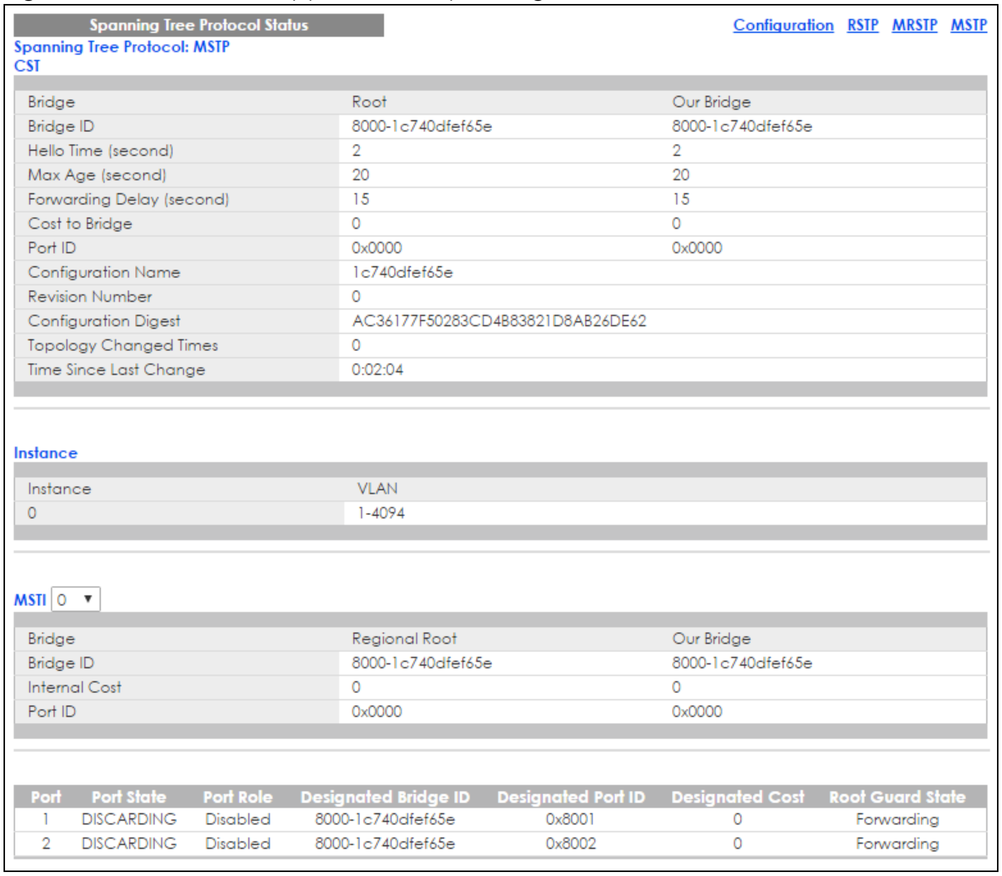
LABEL	DESCRIPTION
MSTP	Click **MSTP** to edit MSTP settings on the Switch.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings 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.
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	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.

13.7 Multiple Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next.

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

Figure 137 Advanced Application > Spanning Tree Protocol > Status: MSTP



The following table describes the labels in this screen.

Table 70 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. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

Table 70   Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	**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.
Port State	This field displays the port state in STP. • **Discarding** – The port does not forward or 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 or 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.

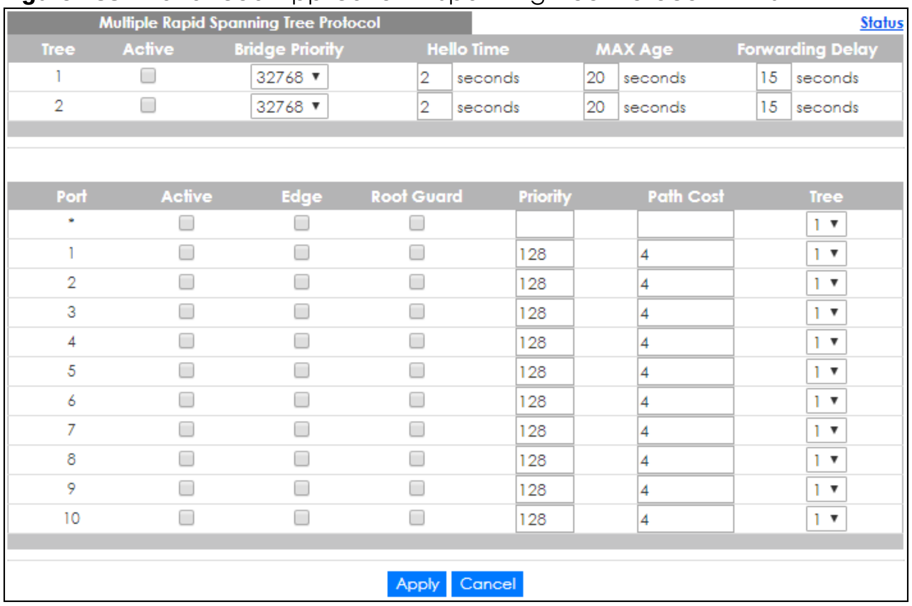
Table 70   Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

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 segment to which this port is connected.
Root Guard State	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 unblocks and allows the port to forward frames again.

13.8 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 13.8 on page 177 for more information on MRSTP.

Figure 138   Advanced Application > Spanning Tree Protocol > MRSTP



The following table describes the labels in this screen.

Table 71   Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MRSTP Status** screen.
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this check box 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.

Table 71 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

LABEL	DESCRIPTION
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate 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).
Root Guard	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.
Tree	Select which STP tree configuration this port should participate in.

Table 71 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

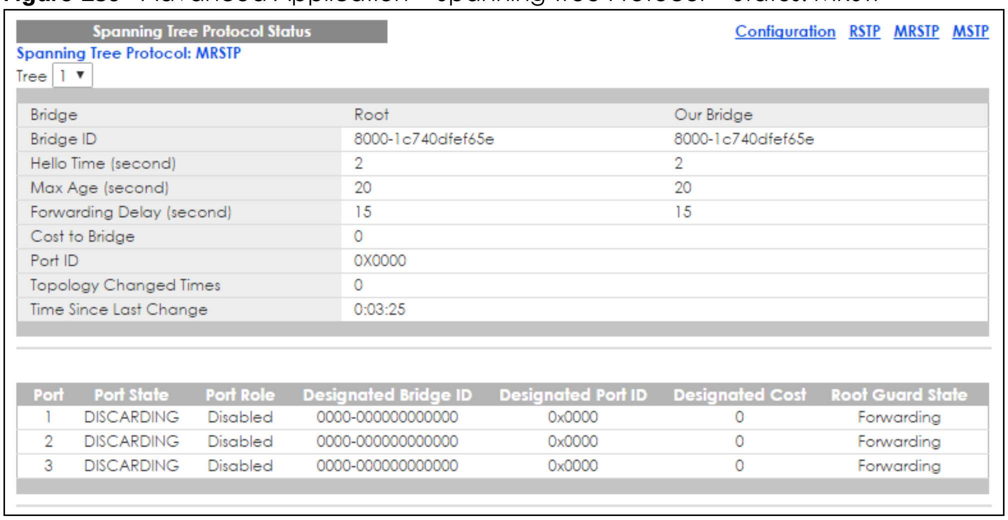
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click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

13.9 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 13.9 on page 179 for more information on MRSTP.

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

Figure 139 Advanced Application > Spanning Tree Protocol > Status: MRSTP



The following table describes the labels in this screen.

Table 72 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) the Switch can wait without receiving a configuration message before attempting to reconfigure.

Table 72 Advanced Application > Spanning Tree Protocol > Status: MRSTP (continued)

LABEL	DESCRIPTION
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 or 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 or 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 segment to which this port is connected.
Root Guard State	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 unblocks and allows the port to forward frames again.

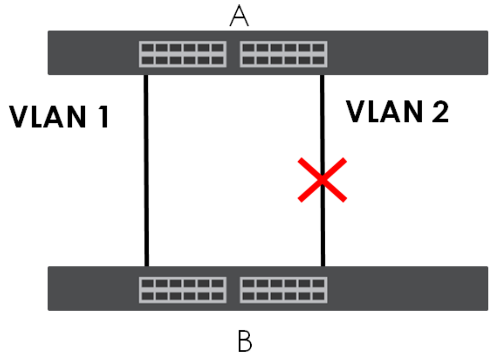
13.10 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

13.10.1 MSTP Network Example

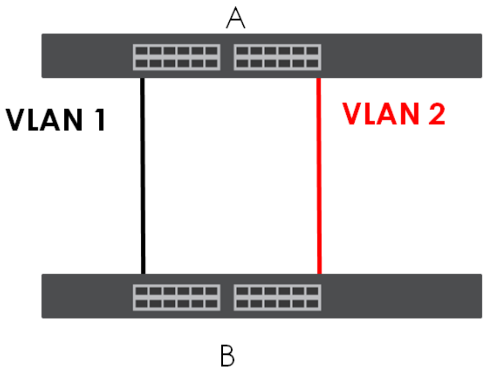
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 140 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 141 MSTP Network Example



13.10.2 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:

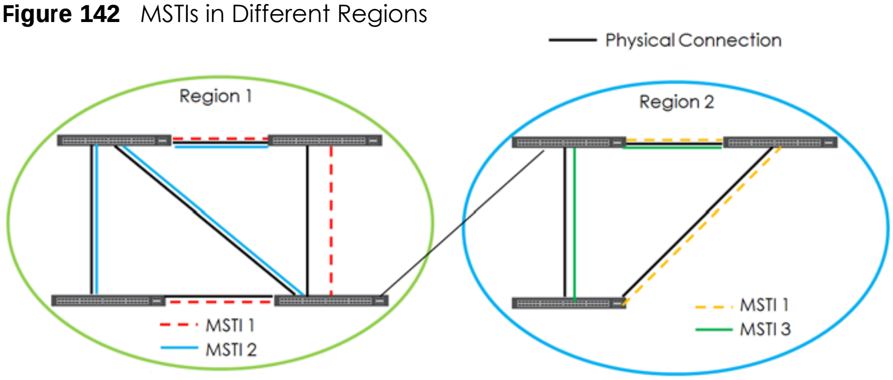
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

13.10.3 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 two spanning tree instances.

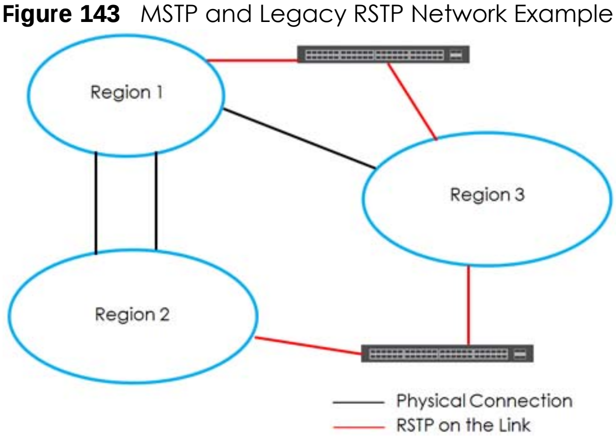
Figure 142 MSTIs in Different Regions



13.10.4 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 143 MSTP and Legacy RSTP Network Example



CHAPTER 14
Bandwidth Control

14.1 Bandwidth Control Overview

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

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

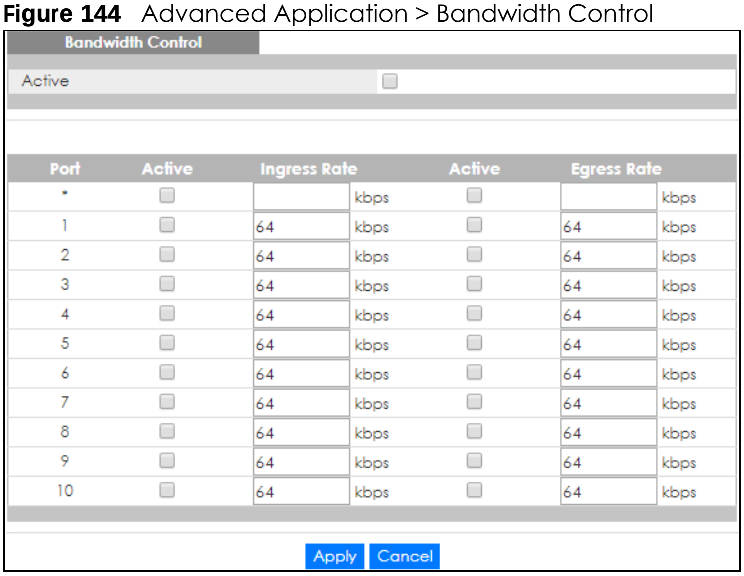
14.1.1 What You Can Do

Use the **Bandwidth Control** screen (Section 14.2 on page 183) to limit the bandwidth for traffic going through the Switch.

14.2 Bandwidth Control Setup

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

Figure 144 Advanced Application > Bandwidth Control



The following table describes the related labels in this screen.

Table 73 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate ingress rate limits on this port.
Ingress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. Note: Ingress rate bandwidth control applies to layer 2 traffic only.
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 reset the fields.

CHAPTER 15
Broadcast Storm Control

15.1 Broadcast Storm Control Overview

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

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.

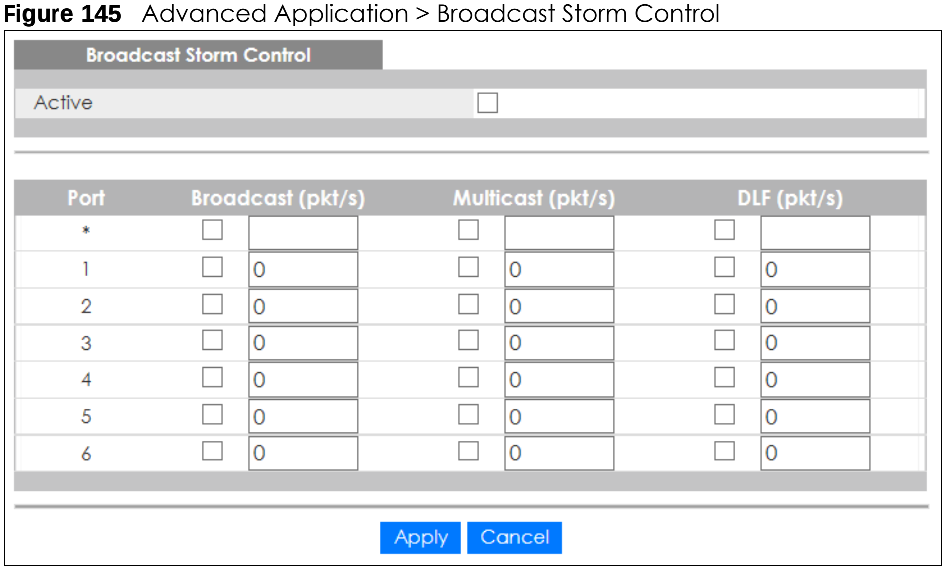
15.1.1 What You Can Do

Use the **Broadcast Storm Control** screen (Section 15.2 on page 185) to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.

15.2 Broadcast Storm Control Setup

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

Figure 145 Advanced Application > Broadcast Storm Control



The following table describes the labels in this screen.

Table 74 Advanced Application > Broadcast Storm Control

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

CHAPTER 16
Mirroring

16.1 Mirroring Overview

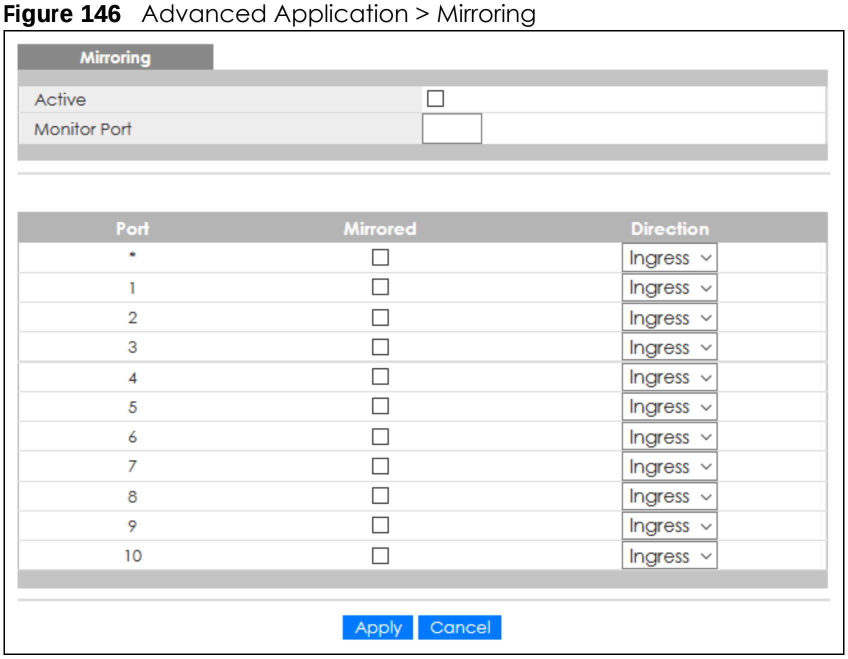
This chapter discusses port mirroring setup screens.

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.

16.2 Port Mirroring Setup

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 146 Advanced Application > Mirroring



The following table describes the labels in this screen.

Table 75   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 ports. Enter the port number of the monitor port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
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 non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

CHAPTER 17 Link Aggregation

17.1 Link Aggregation Overview

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

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.

17.1.1 What You Can Do

- Use the **Link Aggregation Status** screen (Section 17.2 on page 190) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen (Section 17.3 on page 191) to configure static link aggregation.
- Use the **Link Aggregation Control Protocol** screen (Section 17.3.1 on page 193) to enable Link Aggregation Control Protocol (LACP).

17.1.2 What You Need to Know

The Switch supports both static and dynamic link aggregation.

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

See Section 17.4.1 on page 194 for a static port trunking example.

Dynamic Link Aggregation

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

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing 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.

Link Aggregation ID

LACP aggregation ID consists of the following information[1]:

Table 76 Link Aggregation ID: Local Switch

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

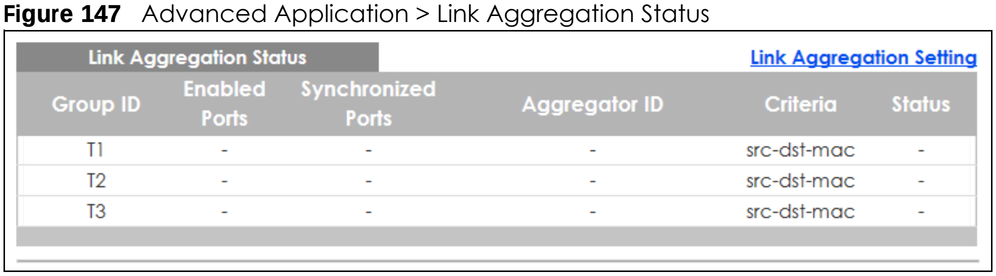
Table 77 Link Aggregation ID: Peer Switch

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

17.2 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See Section 17.1 on page 189 for more information.

Figure 147 Advanced Application > Link Aggregation Status



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

The following table describes the labels in this screen.

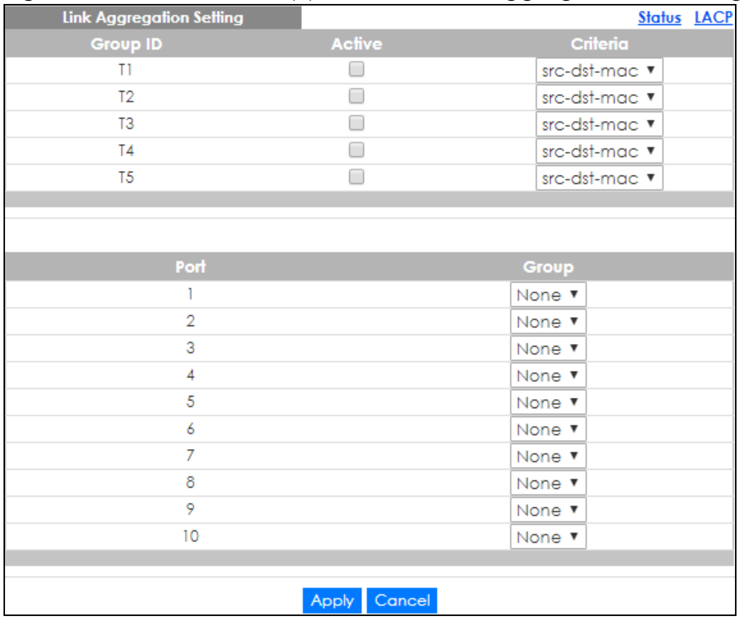
Table 78 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group. The port numbers 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. 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.

17.3 Link Aggregation Setting

Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** to display the screen shown next. See Section 17.1 on page 189 for more information on link aggregation.

Figure 148 Advanced Application > Link Aggregation > Link Aggregation Setting



The following table describes the labels in this screen.

Table 79 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.
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.
Port	This field displays 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.

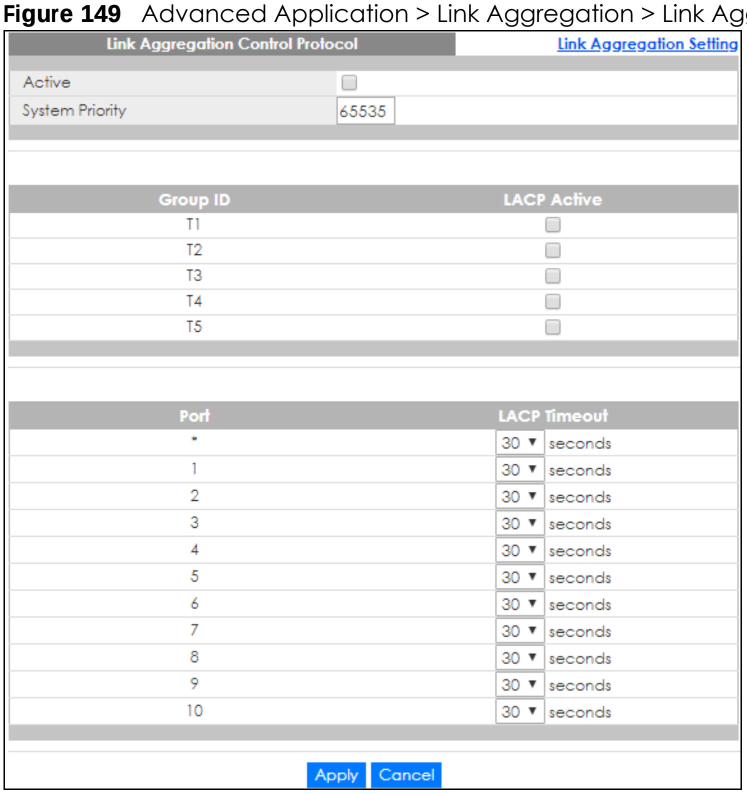
Table 79   Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

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.

17.3.1 Link Aggregation Control Protocol

Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP** to display the screen shown next. See Dynamic Link Aggregation on page 189 for more information on dynamic link aggregation.

Figure 149   Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



The following table describes the labels in this screen.

Table 80   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 check box 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.

Table 80   Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

LABEL	DESCRIPTION
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.
*	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.

17.4 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

17.4.1 Static Trunking Example

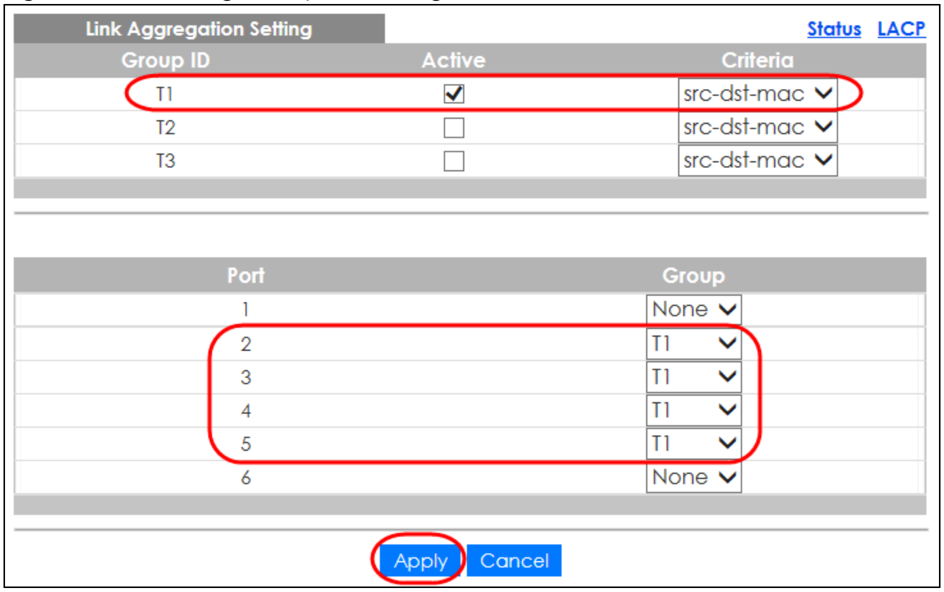
This example shows you how to create a static port trunk group for ports 2 – 5.

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 150   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 151 Trunking Example – Configuration Screen



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

CHAPTER 18
Port Authentication

18.1 Port Authentication Overview

This chapter describes the IEEE 802.1x, MAC, Guest VLAN, and Compound authentication methods.

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**[2] – An authentication server validates access to a port based on a username and password provided by the user.
- **MAC Authentication** – An authentication server validates access to a port based on the MAC address and password of the client.
- **Guest VLAN** – A user that fails an authentication server can still access the port, but traffic from the user is forwarded to the guest VLAN port.
- **Compound Authentication** – An authentication server validates access to a port based on a username and password provided by the user AND/OR MAC address and password of the client.

All types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users.

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

18.1.1 What You Can Do

- Use the **Port Authentication** screen (Section 18.2 on page 198) to display the links to the configuration screens where you can enable the port authentication methods.
- Use the **802.1x** screen (Section 18.3 on page 198) to activate IEEE 802.1x security.
- Use the **MAC Authentication** screen (Section 18.4 on page 199) to activate MAC authentication.
- Use the **Guest Vlan** screen (Section 18.5 on page 201) to enable and assign a guest VLAN to a port.
- Use the **Compound Authentication** screen (Section 18.6 on page 203) to allow network access for clients that pass either IEEE 802.1x authentication OR MAC authentication, or pass both IEEE 802.1x authentication AND MAC authentication.

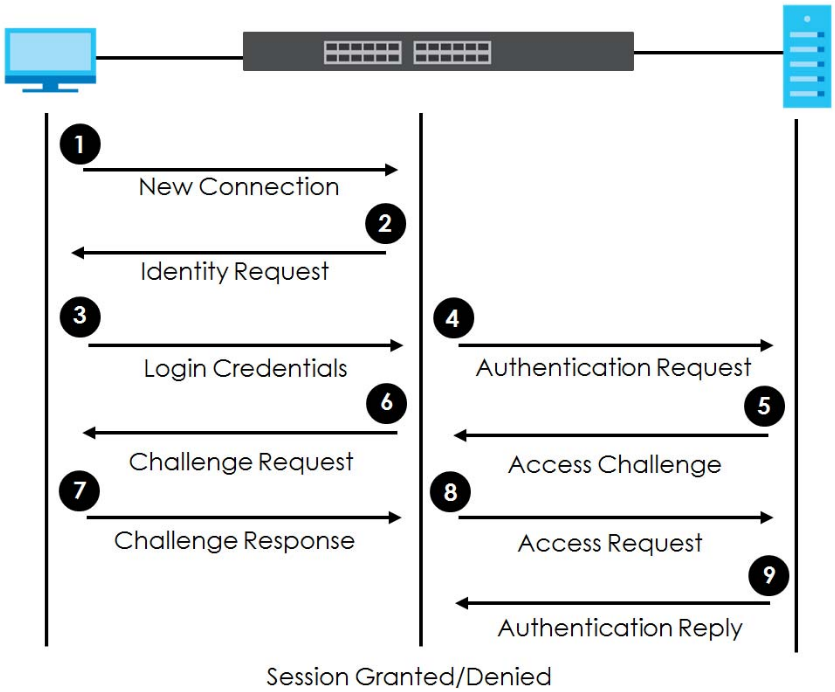
2. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

18.1.2 What You Need to Know

IEEE 802.1x Authentication

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

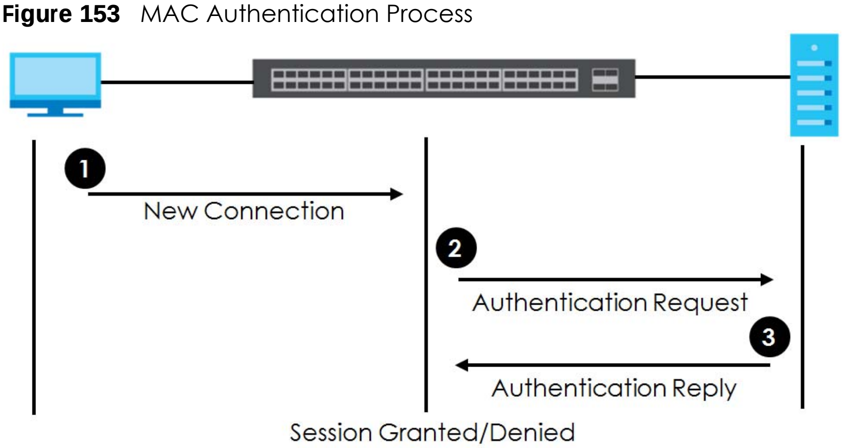
Figure 152 IEEE 802.1x Authentication Process



18.1.3 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 153 MAC Authentication Process

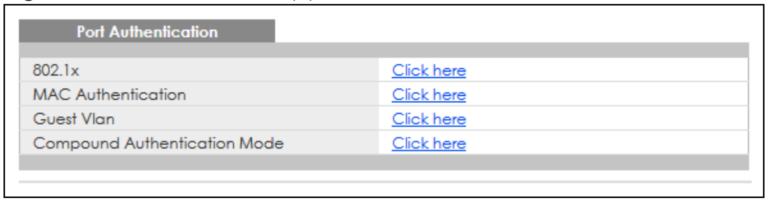


18.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication methods (both on the Switch and the ports), then configure the RADIUS server settings in the **AAA** > **RADIUS Server Setup** screen.

Click **Advanced Application** > **Port Authentication** in the navigation panel to display the screen as shown. Select a port authentication method's link in the screen that appears.

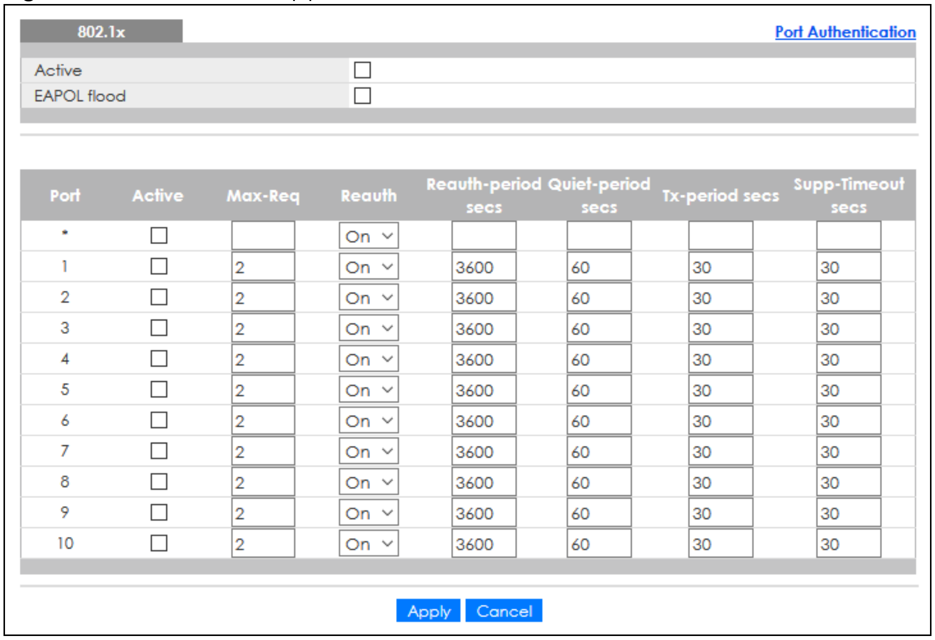
Figure 154 Advanced Application > Port Authentication



18.3 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 155 Advanced Application > Port Authentication > 802.1x



The following table describes the labels in this screen.

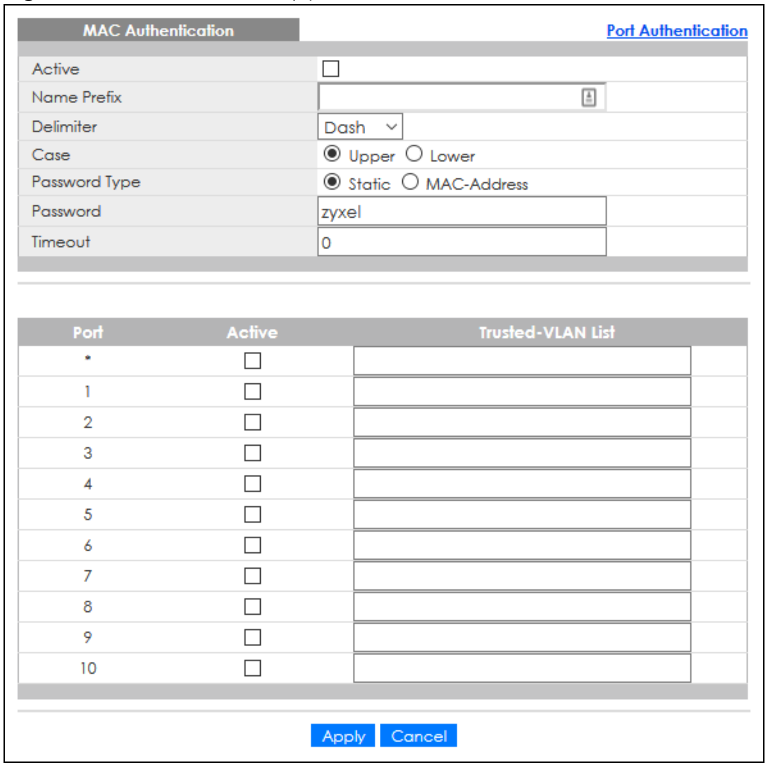
Table 81 Advanced Application > Port Authentication > 802.1x

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.
EAPOL flood	Select this check box to flood EAPoL packets to all ports in the same VLAN. EAP over LAN (EAPOL) is a port authentication protocol used in IEEE 802.1x. It is used to encapsulate and transmit EAP packets between the supplicant (a client device that requests access to the network resources or services) and authenticator (the Switch) directly over the LAN. Note: **EAPOL flood** will not take effect when 802.1x authentication is enabled.
Port	This field displays 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 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 clients 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 secs	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 secs	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 secs	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout secs	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.

18.4 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 156 Advanced Application > Port Authentication > MAC Authentication



The following table describes the labels in this screen.

Table 82 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.
Delimiter	Select the delimiter the RADIUS server uses to separate the pairs in MAC addresses used as the account username (and password). You can select **Dash** (–), **Colon** (:), or **None** to use no delimiters at all in the MAC address.
Case	Select the case (**Upper** or **Lower**) the RADIUS server requires for letters in MAC addresses used as the account username (and password).
Password Type	Select **Static** to have the Switch send the password you specify below or **MAC-Address** to use the client MAC address as the password.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.

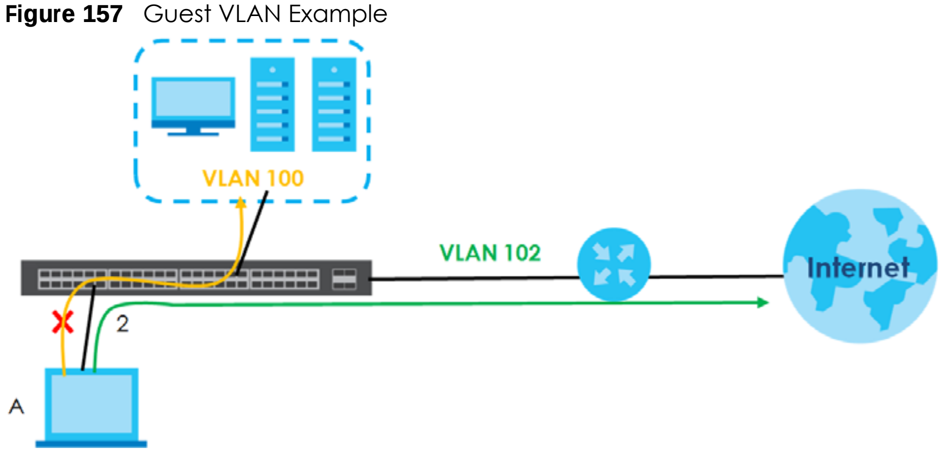
Table 82 Advanced Application > Port Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
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.
Port	This field displays a port number. * means all ports.
*	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	Enter the ID numbers of the trusted VLANs (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.

18.5 Guest VLAN

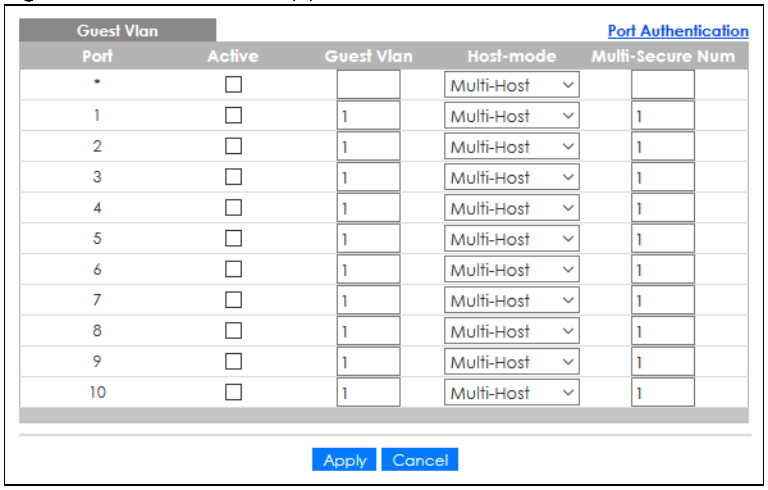
When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the ports. You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in 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 157 Guest VLAN Example



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

Figure 158 Advanced Application > Port Authentication > Guest VLAN



The following table describes the labels in this screen.

Table 83 Advanced Application > Port Authentication > Guest VLAN

LABEL	DESCRIPTION
Port	This field displays a 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. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box 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.
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.

18.6 Compound Authentication

Use this screen to allow network access for clients that:

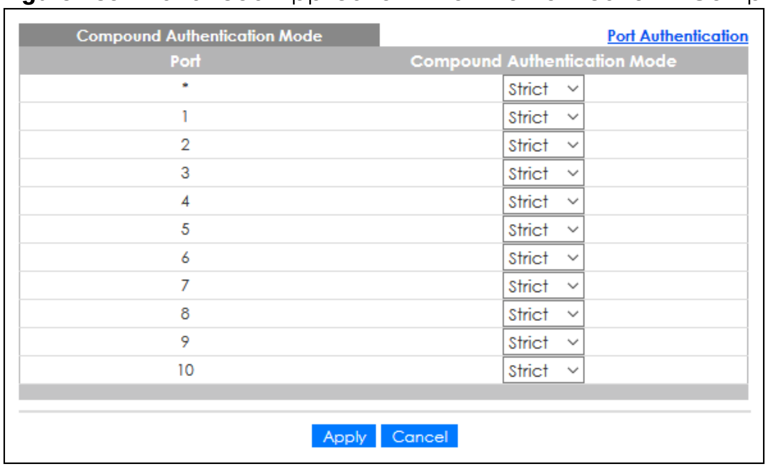
- pass either IEEE 802.1x authentication OR MAC authentication, or
- pass both IEEE 802.1x authentication AND MAC authentication.

The authentication modes are:

- In IEEE 802.1x authentication (Section 18.3 on page 198), the Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port. Use the **AAA** > **RADIUS Server Setup** screen to configure the RADIUS server (Section 25.3 on page 249).
- In MAC authentication (Section 18.4 on page 199), 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.

In the **Port Authentication** screen click **Compound Authentication Mode** to display the configuration screen as shown.

Figure 159 Advanced Application > Port Authentication > Compound Authentication Mode



The following table describes the labels in this screen.

Table 84 Advanced Application > Port Authentication > Compound Authentication Mode

LABEL	DESCRIPTION
Port	This field displays a 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. Changes in this row are copied to all the ports as soon as you make them.
Compound Authentication Mode	Specify how the Switch authenticates clients for network access. Select **Strict** to allow network access to clients only when clients passes IEEE 802.1x authentication AND MAC authentication at the same time. Select **Loose** to allow network access to clients when clients passes IEEE 802.1x authentication OR MAC authentication.

Table 84 Advanced Application > Port Authentication > Compound Authentication Mode (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.

CHAPTER 19
Port Security

This chapter shows you how to set up port security.

19.1 About Port Security

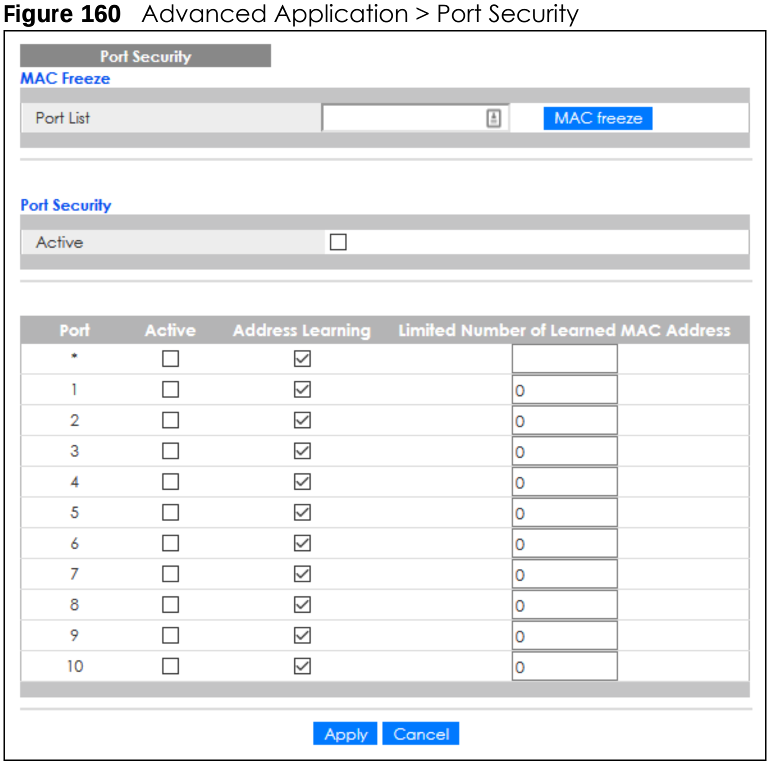
Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 32K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 32K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC addresses 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.

19.2 Port Security Setup

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

Figure 160 Advanced Application > Port Security



The following table describes the labels in this screen.

Table 85   Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the ports (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click **MAC freeze**, all previously learned MAC addresses on the specified ports 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.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some 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 addresses is in the MAC address table on this port. Packets with no matching MAC addresses 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.

CHAPTER 20
Time Range

20.1 Time Range Overview

You can set up one-time and recurring schedules for time-oriented features, such as PoE and classifier. The UAG supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the Switch.

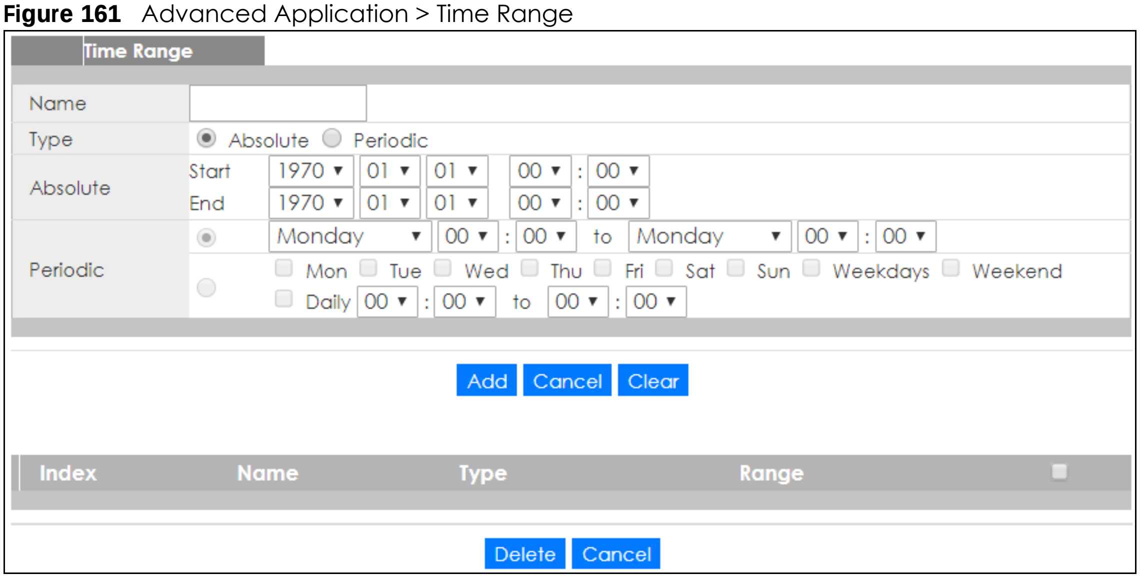
20.1.1 What You Can Do

Use the **Time Range** screen (Section 20.2 on page 207) to view or define a schedule on the Switch.

20.2 Configuring Time Range

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

Figure 161 Advanced Application > Time Range



The following table describes the labels in this screen.

Table 86 Advanced Application > Time Range

LABEL	DESCRIPTION
Name	Enter a descriptive name for this rule for identifying purposes.
Type	Select **Absolute** to create a one-time schedule. One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods. Alternatively, select **Periodic** to create a recurring schedule. Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules are useful for defining the workday and off-work hours.
Absolute	This section is available only when you set **Type** to **Absolute**.
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 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 clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Type	This field displays the type of the schedule.
Range	This field displays the time periods 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 rules that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

CHAPTER 21 Classifier

21.1 Classifier Overview

This chapter introduces and shows you how to configure the packet classifier on the Switch. It also discusses Quality of Service (QoS) and classifier concepts as employed by the Switch.

21.1.1 What You Can Do

- Use the **Classifier Status** screen (Section 21.2 on page 210) to view the classifiers configured on the Switch and how many times the traffic matches the rules.
- Use the **Classifier Configuration** screen (Section 21.3 on page 210) to define the classifiers and view a summary of the classifier configuration. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.
- Use the **Classifier Global Setting** screen (Section 21.4 on page 215) to configure the match order and enable logging on the Switch.

21.1.2 What You Need to Know

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

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

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

1 Configure classifiers to sort traffic into different flows.

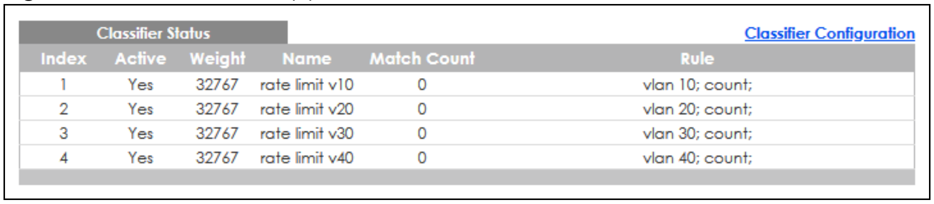
2 Configure policy rules to define actions to be performed on a classified traffic flow (refer to Chapter 22 on page 218 to configure policy rules).

21.2 Classifier Status

Use this screen 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 162 Advanced Application > Classifier > Classifier Status



The following table describes the labels in this screen.

Table 87 Advanced Application > Classifier

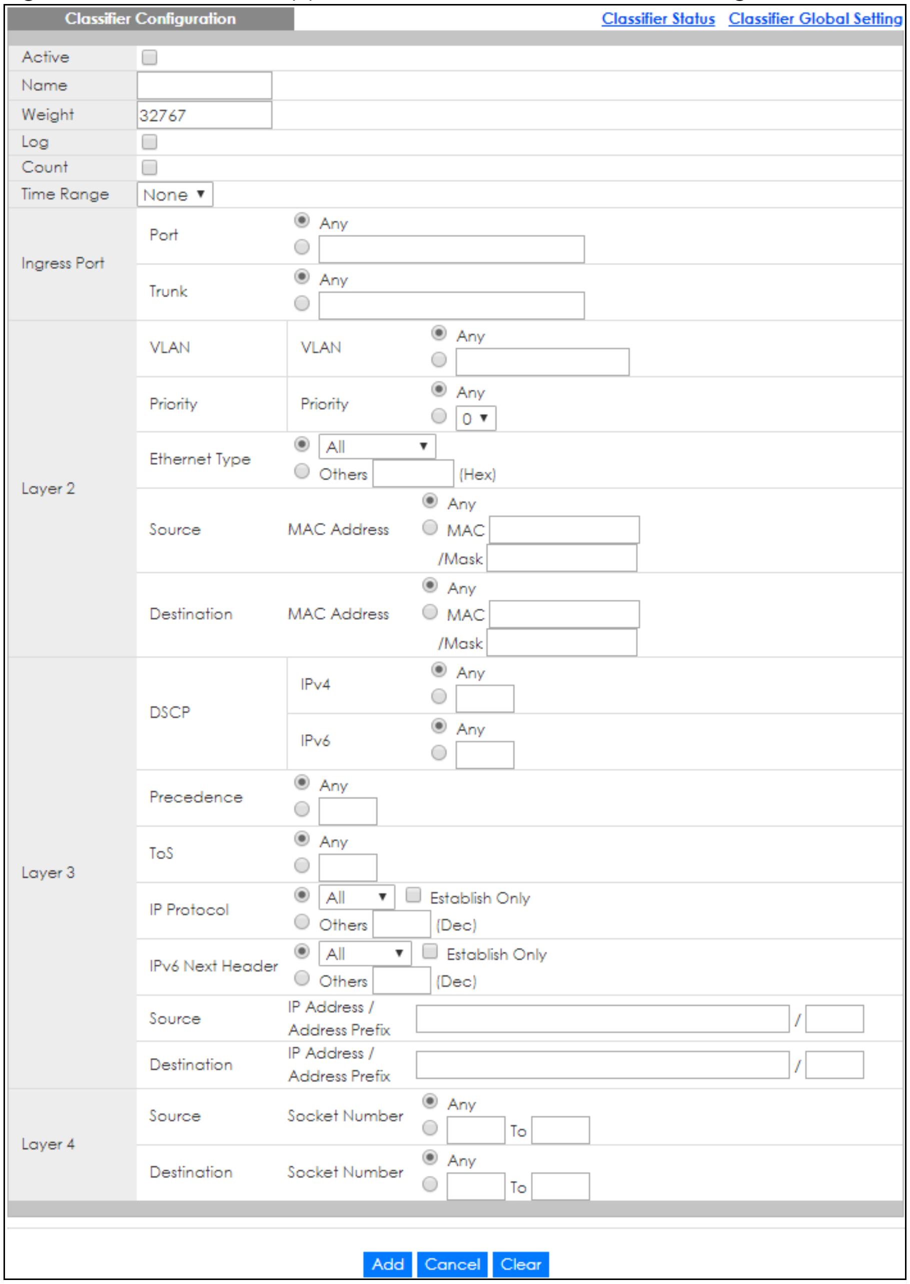
LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Weight	This field displays the rule's weight. This is to indicate a rule's priority when the match order is set to **manual** in the **Classifier** > **Classifier Configuration** > **Classifier Global Setting** screen. The higher the number, the higher the rule's priority.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
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.
Clear	Select **Classifie**r, enter a classifier rule name and then click **Clear** to erase the recorded statistical information for the classifier, or select **Any** to clear statistics for all classifiers.

21.3 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 163 Advanced Application > Classifier > Classifier Configuration



The following table describes the labels in this screen.

Table 88 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.
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.

Table 88 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
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.
Time Range	Select the name of the pre-configured 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.
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.
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.
Ethernet Type	Select an Ethernet type or select **Other** and enter the Ethernet type number in hexadecimal value.
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 bits of the matched traffic's MAC address, which can be of any hexadecimal characters. 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	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select **MAC/Mask** to enter the destination 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 bits of the matched traffic's MAC address, which can be of any hexadecimal characters. 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.	

Table 88 Advanced Application > Classifier > Classifier Configuration (continued)

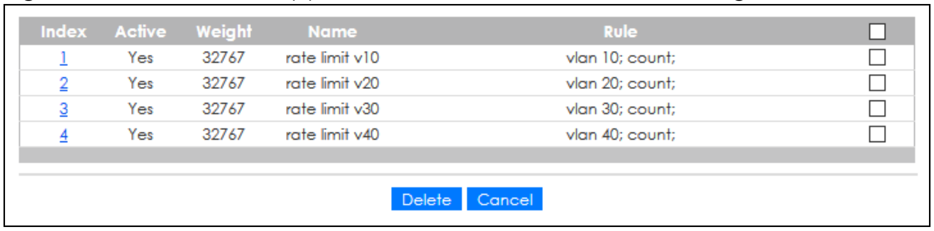
LABEL	DESCRIPTION
DSCP IPv4/IPv6	Select **Any** to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Precedence	Select **Any** to classify traffic from any precedence or select the second option and specify an IP Precedence (the first 3 bits of 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. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will pick out the packets that are sent to 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. A subnet mask can be represented in a 32-bit notation. For example, the subnet mask “255.255.255.0” can be represented as “11111111.11111111.11111111.00000000”, and counting up the number of ones in this case results in 24.
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 4 classifier.	
Source	
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.
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.
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 back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

21.3.1 Viewing and Editing Classifier Configuration Summary

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

Note: When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 164 Advanced Application > Classifier > Classifier Configuration: Summary Table



The following table describes the labels in this screen.

Table 89 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 purpose 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 90 Common Ethernet Types and Protocol Numbers

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In the Internet Protocol there is a field, called "Protocol", to identify the next level protocol. The following table shows some common protocol types and the corresponding protocol number. Refer to http://www.iana.org/assignments/protocol-numbers for a complete list.

Table 91 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

Some of the most common TCP and UDP port numbers are:

Table 92 Common TCP and UDP Port Numbers

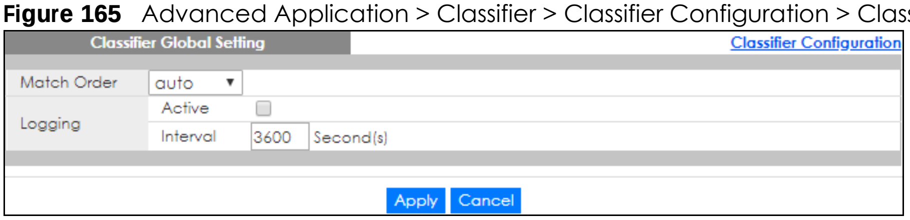
PROTOCOL NAME	TCP/UDP PORT NUMBER
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110

See Appendix B on page 530 for information on commonly used port numbers.

21.4 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 165 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting



The following table describes the labels in this screen.

Table 93 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting

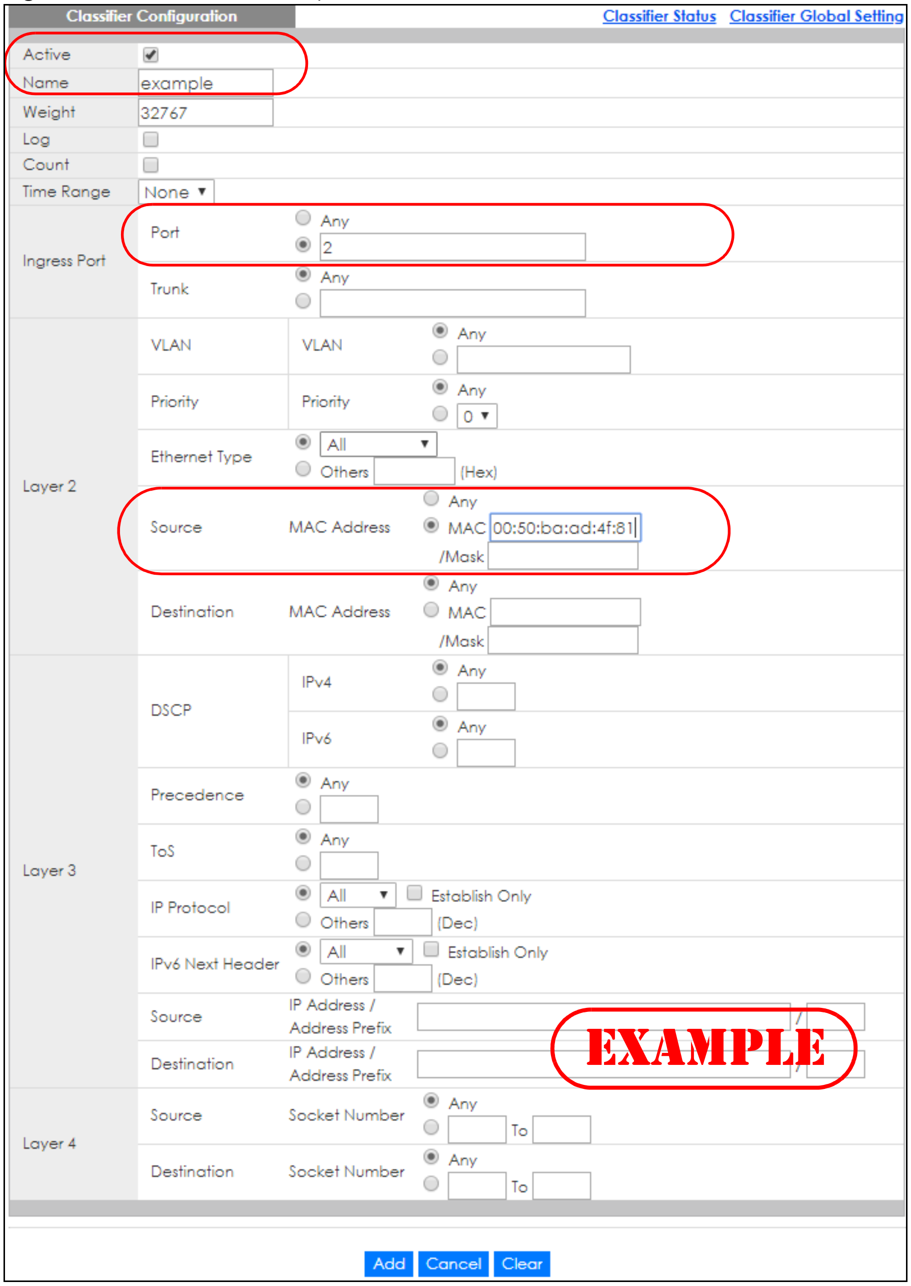
LABEL	DESCRIPTION
Match Order	Select **manual** to have classifier rules applied according to the weight of each rule you configured in **Advanced Application** > **Classifier** > **Classifier Configuration**. Alternatively, select **auto** to have classifier rules applied according to the layer of the 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 classifier A.
Logging	
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.

21.5 Classifier Example

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

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define actions on the classified traffic flow.

Figure 166 Classifier: Example



CHAPTER 22
Policy Rule

22.1 Policy Rules Overview

This chapter shows you how to configure policy rules.

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 21 on page 209 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

22.1.1 What You Can Do

Use the **Policy Rule** screen (Section 22.2 on page 219) to enable the policy and display the active classifiers you configure in the **Classifier** screen.

22.1.2 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.

22.1.3 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.

DSCP (6 bits)	Unused (2 bits)

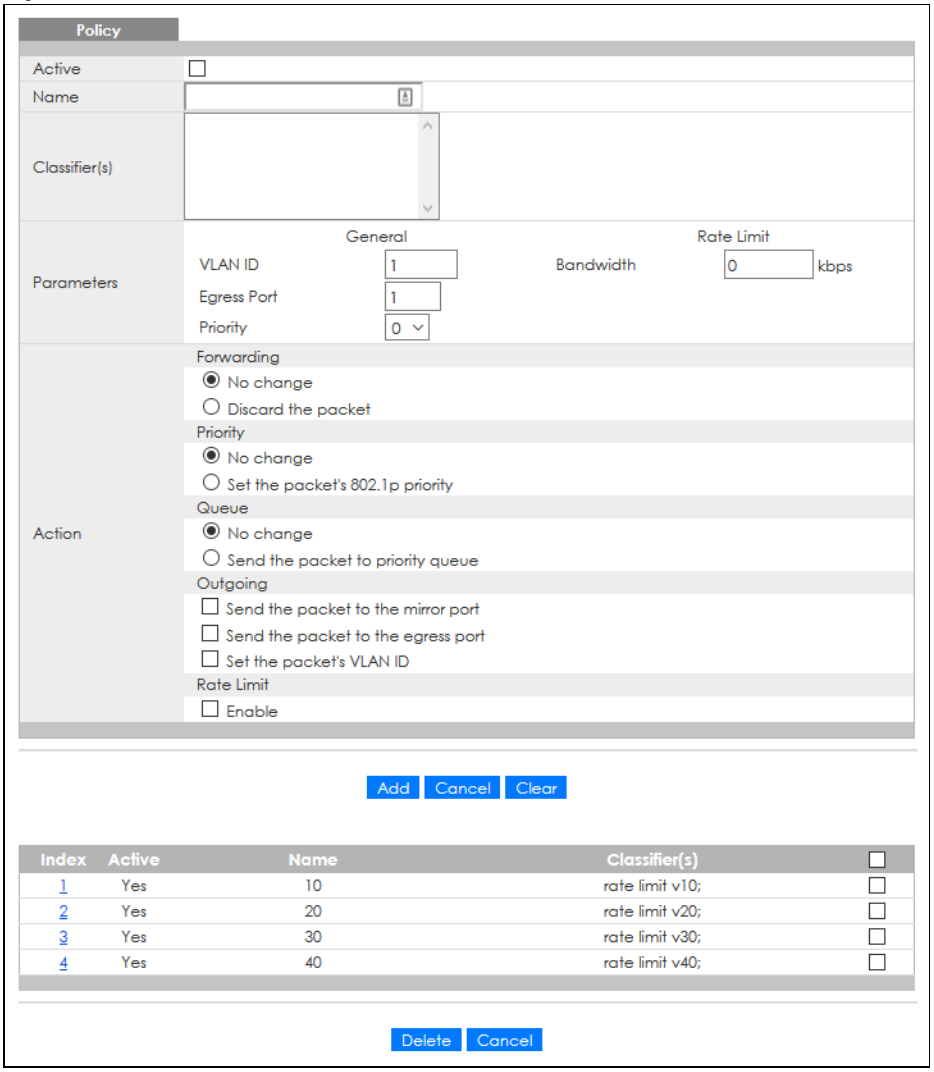
The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the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

22.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen.

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

Figure 167 Advanced Application > Policy Rule



The following table describes the labels in this screen.

Table 94 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 classifiers you configure in the **Classifier** screen. Select the classifiers to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the fields that is related to the actions you configure in the **Action** field.	

Table 94 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
General	
VLAN ID	Specify a VLAN ID.
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.
Rate Limit	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.
Action Specify the actions the Switch takes on the associated classified traffic flow. Note: You can specify only one action (pair) in a policy rule. To have the Switch take multiple actions on the same traffic flow, you need to define multiple classifiers with the same criteria and apply different policy rules. Say you have several classifiers that identify the same traffic flow and you specify a different policy rule for each. If their policy actions conflict (**Discard the packet**, **Send the packet to the egress port** and **Rate Limit**), the Switch only applies the policy rules with the **Discard the packet** and **Send the packet to the egress port** actions depending on the classifier names. The longer the classifier name, the higher the classifier priority. If two classifier names are the same length, the bigger the character, the higher the classifier priority. The lowercase letters (such as a and b) have higher priority than the capitals (such as A and B) in the classifier name. For example, the classifier with the name of class 2, class a or class B takes priority over the classifier with the name of class 1 or class A. Let's say you set two classifiers (Class 1 and Class 2) and both identify all traffic from MAC address 11:22:33:44:55:66 on port 3. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to forward the packets to the egress port, the Switch will forward the packets. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will discard the packets immediately. If Policy 1 applies to Class 1 and the action is to forward the packets to the egress port, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will forward the packets.	
Forwarding	Select **No change** to forward the packets. Select **Discard the packet** to drop the packets.
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.
Queue	Select **No change** to follow the priority queue setting in **Basic Setting** > **Switch Setup** > **Priority Queue Assignment**. Select **Send the packet to priority queue** to send the packet to the specific priority queue with the value you set in the **Priority** 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. Select **Set the packet's VLAN ID** to set the packet's VLAN ID.
Rate Limit	Select **Enable** to activate bandwidth limitation on the traffic flows then set the actions to be taken on out-of-profile packets.
Add	Click **Add** to inset the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.

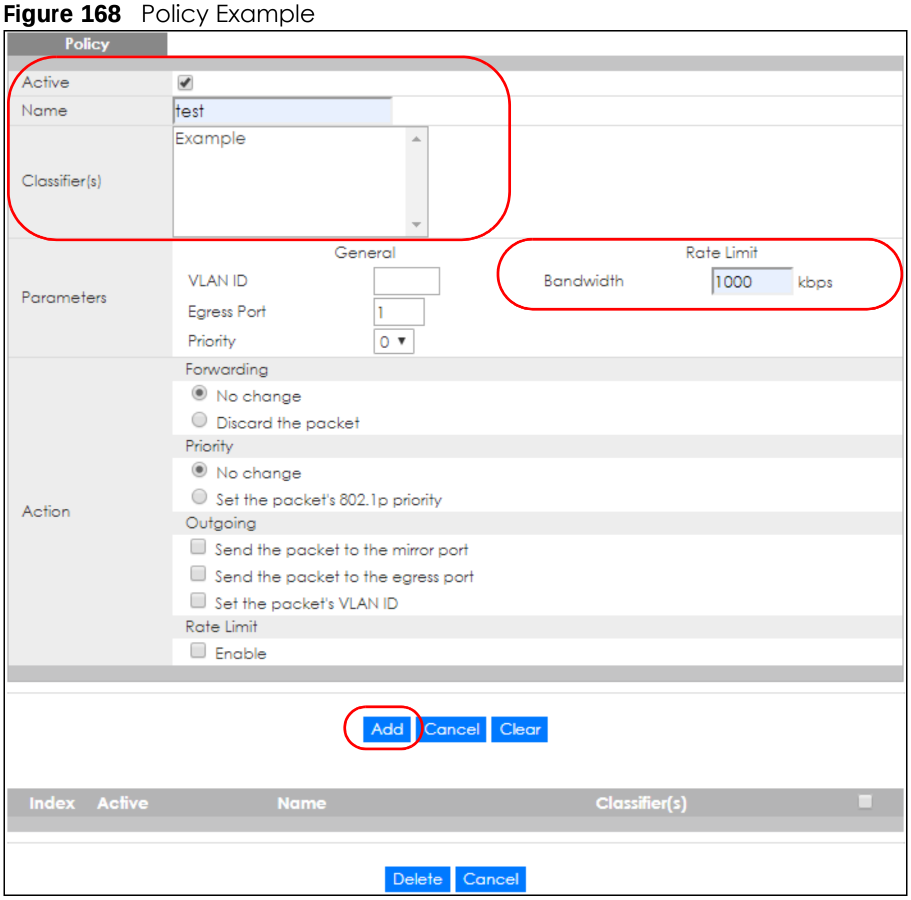
Table 94   Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
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 names 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.

22.3 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 21.5 on page 216).

Figure 168   Policy Example



CHAPTER 23
Queuing Method

23.1 Queuing Method Overview

This chapter introduces the queuing methods supported.

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.

23.1.1 What You Can Do

Use the **Queuing Method** screen (Section 23.2 on page 223) set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

23.1.2 What You Need to Know

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SPQ does not automatically adapt to changing network requirements.

Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (portion) (the number you configure in the Weight field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

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 a 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.

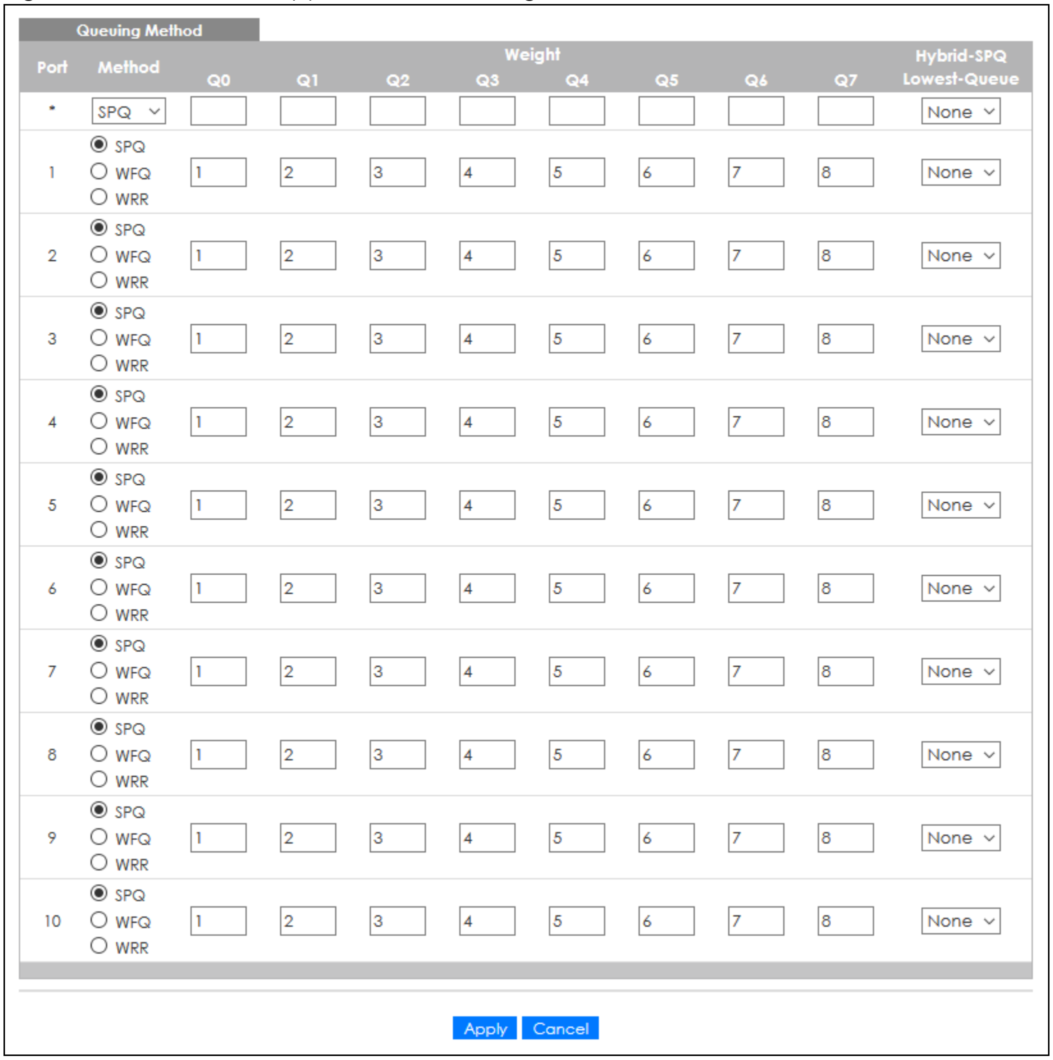
Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than 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.

23.2 Configuring Queuing

Use this screen to set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

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

Figure 169 Advanced Application > Queuing Method



The following table describes the labels in this screen.

Table 95 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Method	Select **SPQ** (Strictly Priority Queuing), **WFQ** (Weighted Fair Queuing) or **WRR** (Weighted Round Robin). Strictly Priority Queuing 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 portion (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	When you select **WFQ** or **WRR** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
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 queues after and including the specified queue for the port. 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** for 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.

CHAPTER 24 Multicast

24.1 Multicast Overview

This chapter shows you how to configure various multicast features.

Traditionally, IP packets are transmitted in one of either two ways – Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group – it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

24.1.1 What You Can Do

- Use the **Multicast Setup** screen (Section 24.2 on page 229) to display the links to the configuration screens where you can configure IPv4 multicast settings.
- Use the **IPv4 Multicast Status** screen (Section 24.3 on page 229) to view multicast group information.
- Use the **IGMP Snooping** screen (Section 24.3.1 on page 230) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IGMP Snooping VLAN** screen (Section 24.3.2 on page 233) to perform IGMP snooping on up to 16 VLANs.
- Use the **IGMP Filtering Profile** (Section 24.3.3 on page 234) to specify a range of multicast groups that clients connected to the Switch are able to join.
- Use the **IPv6 Multicast Status** screen (Section 24.4 on page 236) to view multicast group information.
- Use the **MLD Snooping-proxy** screen (Section 24.4.1 on page 236) to enable the upstream port to report group changes to a connected multicast router and forward MLD messages to other upstream ports.
- Use the **MVR** screens (Section 24.5 on page 242) to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN.

24.1.2 What You Need to Know

Read on for concepts on Multicasting that can help you configure the screens in this chapter.

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).

IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers or 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.

IGMP Snooping and VLANs

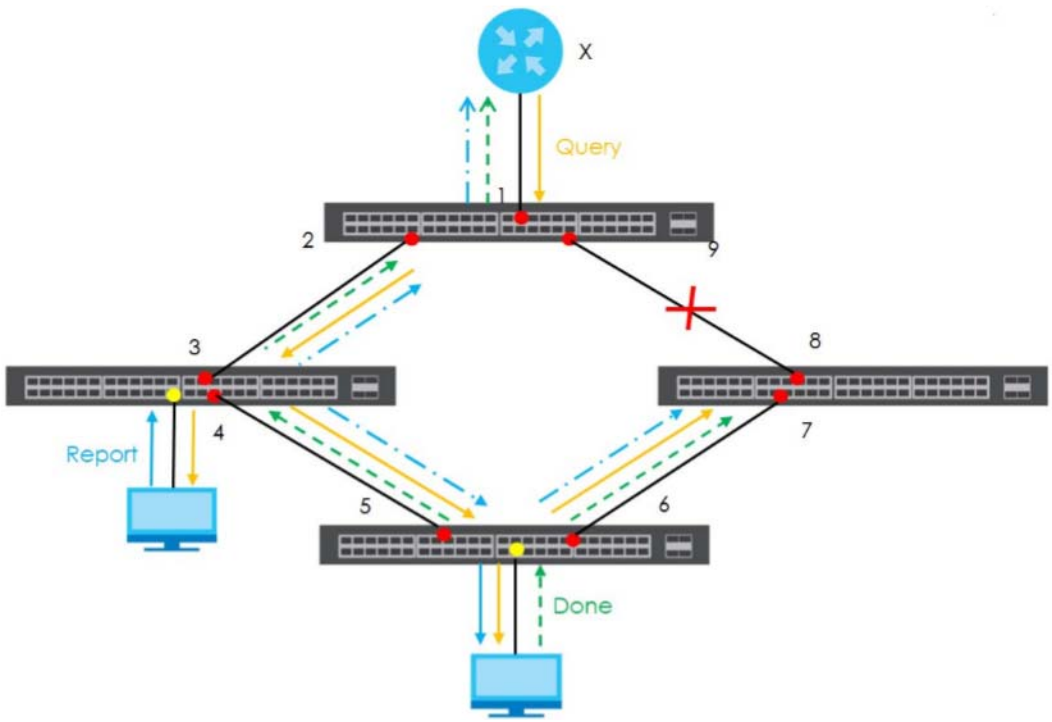
The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the 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.

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.



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.

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 170 MVR Network Example

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.

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.

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.

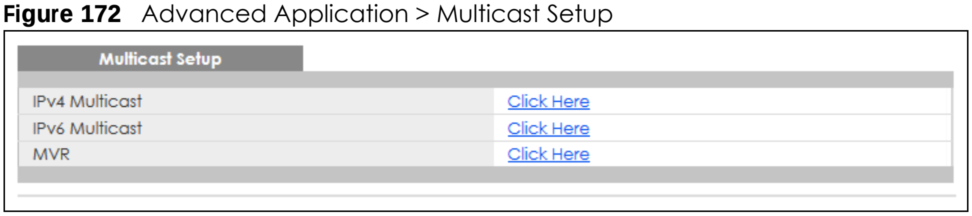
When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, an uplink port on the Switch). If there is another subscriber device connected to this port 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 171 MVR Multicast Television Example

24.2 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 172 Advanced Application > Multicast Setup



The following table describes the labels in this screen.

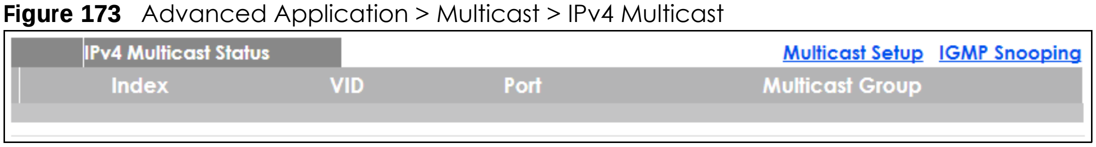
Table 96 Advanced Application > Multicast Setup

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-proxy and MLD filtering for IPv6.
MVR	Click the link to open screens where you can create multicast VLANs.

24.3 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 24.1 on page 225 for more information on multicasting.

Figure 173 Advanced Application > Multicast > IPv4 Multicast



The following table describes the labels in this screen.

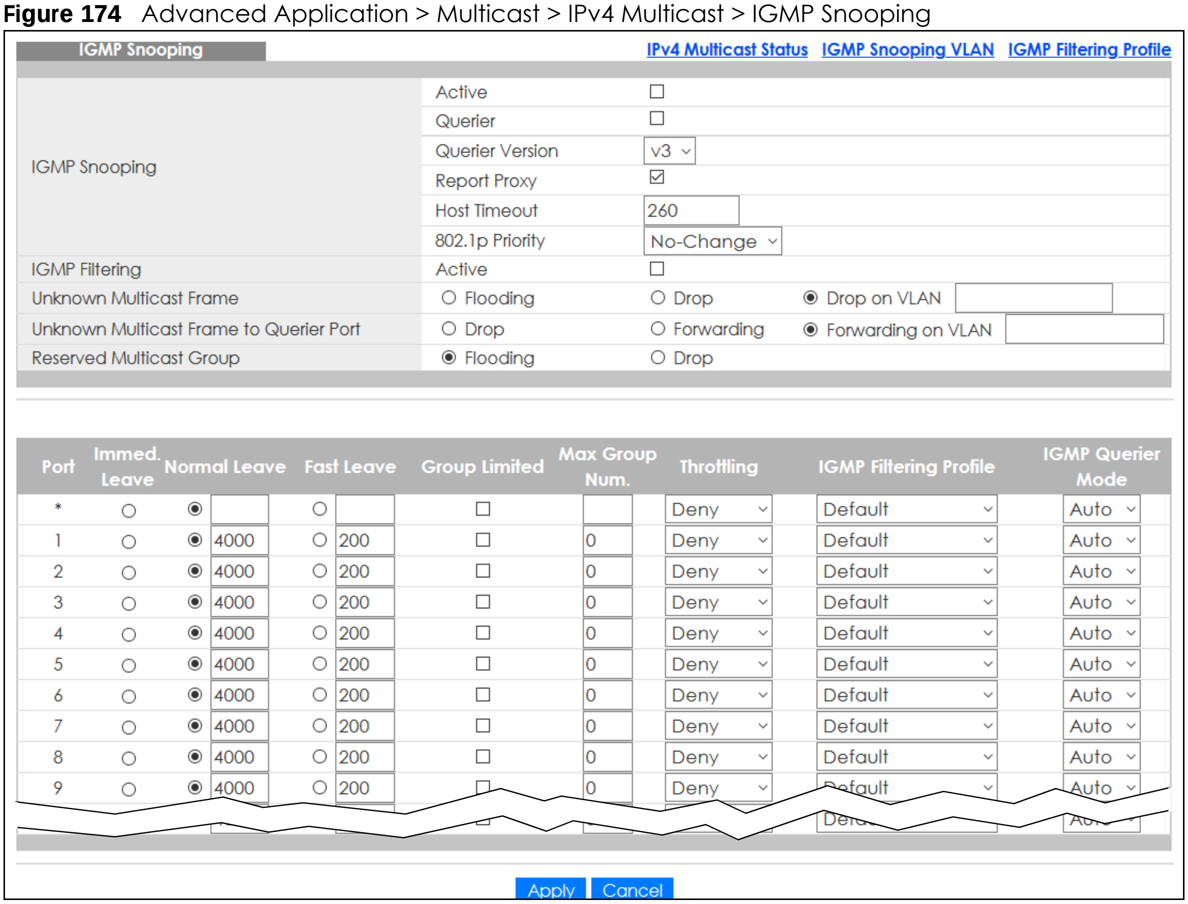
Table 97   Advanced Application > Multicast > IPv4 Multicast

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.
Multicast Group	This field displays IP multicast group addresses.

24.3.1 IGMP Snooping

Click the **IGMP Snooping** link in the **Advanced Application** > **Multicast** > **IPv4 Multicast** screen to display the screen as shown. See Section 24.1 on page 225 for more information on multicasting.

Figure 174   Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping



The following table describes the labels in this screen.

Table 98   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.

Table 98 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Querier Version	IGMP snooping query works only when both host and Switch support the same IGMP version. Select **v2** to allow the Switch to send IGMPv2 queries only. Select **v3** to allow the Switch to send IGMPv3 queries only.
Report Proxy	Select this option to allow the Switch to act as the IGMP report proxy and leave proxy. It will report group changes to a connected multicast router. The Switch not only checks IGMP packets between multicast routers or switches and multicast hosts to learn the multicast group membership, but also replaces the source MAC address in an IGMP v1/v2 report with its own MAC address before forwarding to the multicast router or switch. When the Switch receives more than one IGMP v1/v2 join report that requests to join the same multicast group, it only sends a new join report with its MAC address. This helps reduce the number of multicast join reports passed to the multicast router or switch. The Switch sends a leave message with its MAC address to the multicast router or switch only when it receives the leave message from the last host in a multicast group.
Host Timeout	Specify the time (from 1 to 16711450) 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. 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 frames. • Select **Flooding** to send the frames to all ports. • Select **Drop on VLAN** and enter the VLAN ID numbers to discard the frames on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
Unknown Multicast Frame to Querier Port	Specify the action to perform when **Unknown Multicast Frame** is set to **Drop**. • Select **Drop** to discard the frames. • Select **Forwarding** to send the frames to all querier ports. • Select **Forwarding on VLAN** and enter the VLAN ID numbers to send the frames to the ports which are used as an IGMP query port on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
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 frames. • Select **Flooding** to send the frames to all ports.
Port	This field displays the port number.

Table 98 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (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. 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.
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6348800) 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 6348800) 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 frames 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 reports 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.

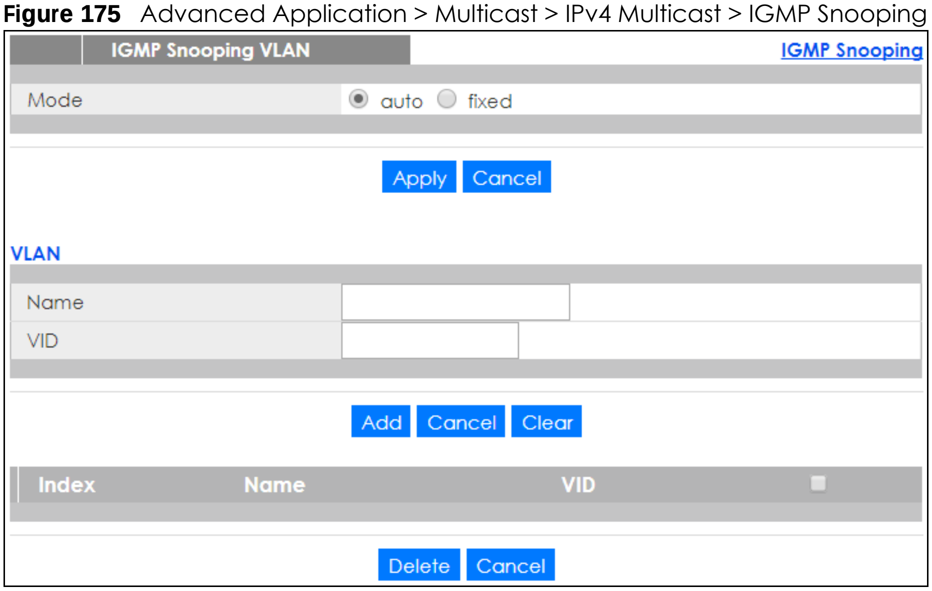
Table 98 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
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.

24.3.2 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 IGMP Snooping and VLANs on page 226 for more information on IGMP Snooping VLAN.

Figure 175 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN



The following table describes the labels in this screen.

Table 99 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

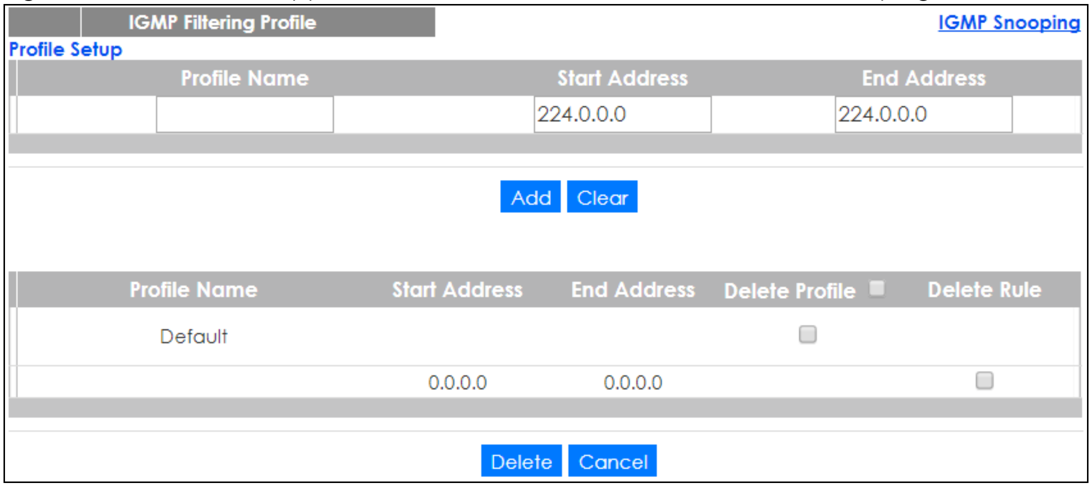
LABEL	DESCRIPTION
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLANs that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. 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.
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. Click on an index number to view more details or change the settings.
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 entries that you want to remove, then click the **Delete** button.
Cancel	Click **Cancel** to clear the check boxes.

24.3.3 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 176 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile



The following table describes the labels in this screen.

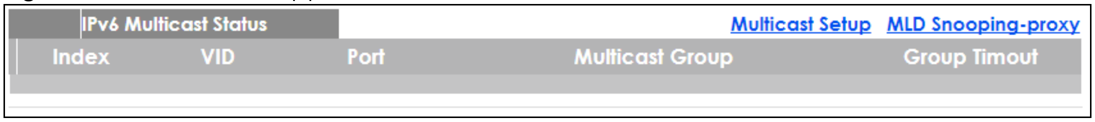
Table 100 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rules 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 boxes of the rules that you want to remove from a profile.
Delete	To delete the profiles and all the accompanying rules, select the profiles that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rules from a profile, select the rules that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile** or **Delete Rule** check boxes.

24.4 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 24.1 on page 225 for more information on multicasting.

Figure 177 Advanced Application > Multicast > IPv6 Multicast



The following table describes the fields in the above screen.

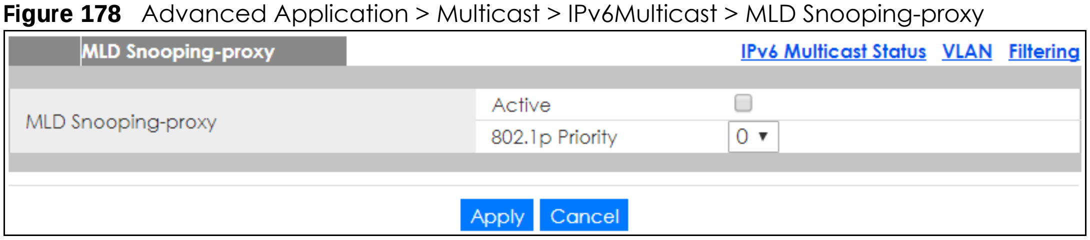
Table 101 Advanced Application > Multicast > IPv6 Multicast

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.
Multicast Group	This field displays IP multicast group addresses.
Group Timeout	This field displays the time (in seconds) that elapses before the Switch removes a MLD group membership entry if it does not receive report messages from the port.

24.4.1 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 24.1 on page 225 for more information on multicasting.

Figure 178 Advanced Application > Multicast > IPv6Multicast > MLD Snooping-proxy



The following table describes the fields in the above screen.

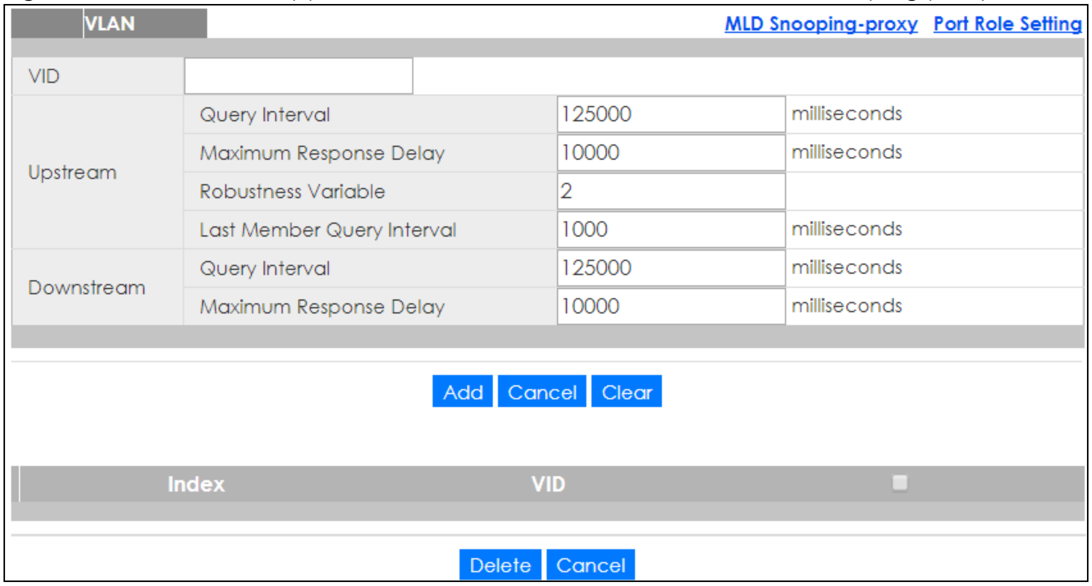
Table 102 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy

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.

24.4.2 MLD Snooping-proxy VLAN

Click the **VLAN** link in the **Advanced Application** > **Multicast** > **IPv6 Multicast** > **MLD Snooping-proxy** screen to display the screen as shown. See Section 24.1 on page 225 for more information on multicasting.

Figure 179 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN



The following table describes the fields in the above screen.

Table 103 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 is 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 is 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**.

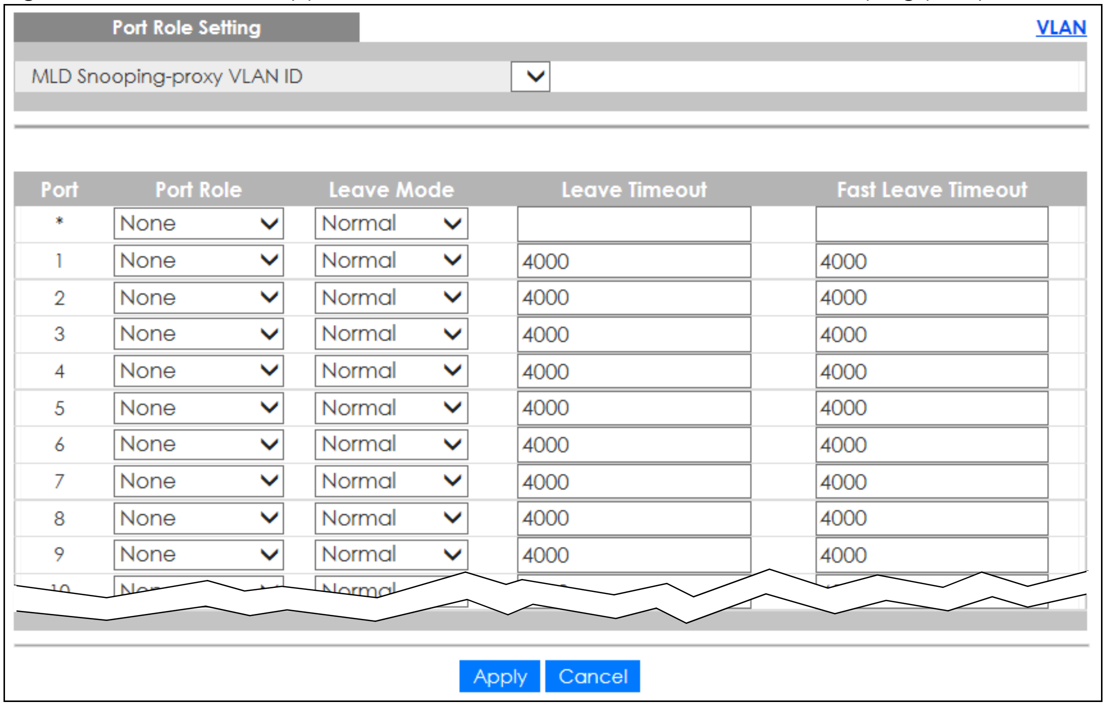
Table 103   Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

LABEL	DESCRIPTION
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.
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 entries permanently.
Cancel	Click **Cancel** to clear the check boxes.

24.4.3 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 24.1 on page 225 for more information on multicasting.

Figure 180 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Port Role Setting



The following table describes the fields in the above screen.

Table 104 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > 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.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. 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 ports 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 ports. 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.

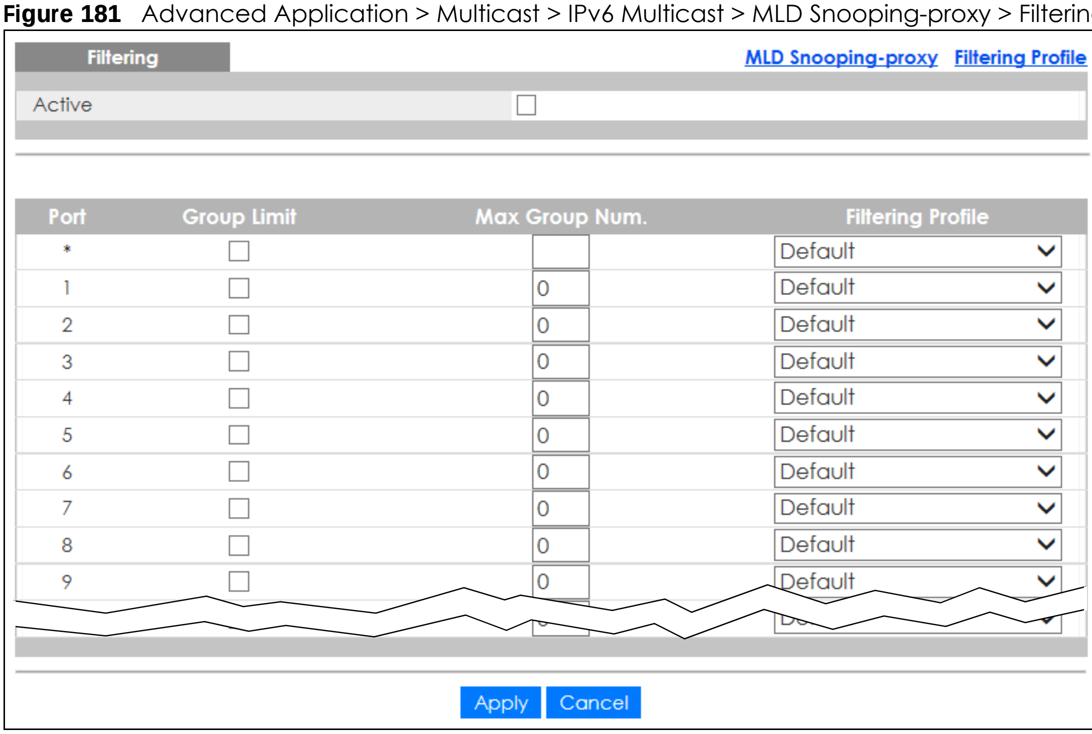
Table 104 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Port Role Setting

LABEL	DESCRIPTION
Fast Leave Timeout	Enter the fast leave timeout (in milliseconds) for the specified downstream ports. 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.

24.4.4 MLD Snooping-proxy Filtering

Use this screen to configure the Switch's MLD filtering settings. Click the **Filtering** link in the **Advanced Application** > **Multicast** > **IPv6 Multicast** > **MLD Snooping-proxy** screen to display the screen as shown.

Figure 181 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering



The following table describes the fields in the above screen.

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

LABEL	DESCRIPTION
Active	Select this option to enable MLD filtering on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. 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.

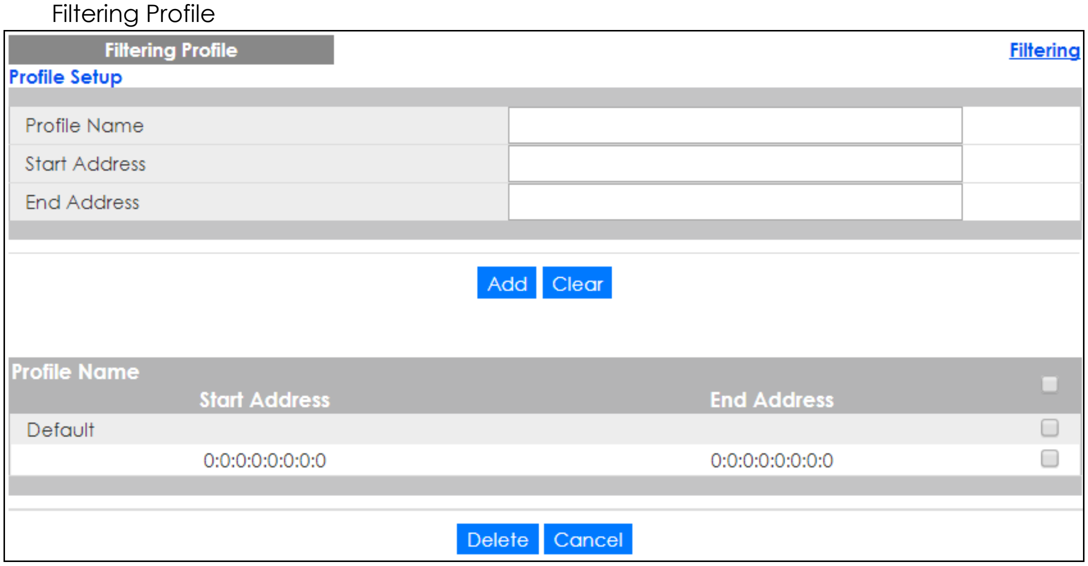
Table 105 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering

LABEL	DESCRIPTION
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.

24.4.5 MLD Snooping-proxy Filtering Profile

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

Figure 182 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile



The following table describes the fields in the above screen.

Table 106 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rules 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.

Table 106 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering Profile

LABEL	DESCRIPTION
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 profiles and all the accompanying rules, select the profiles 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 rules from a profile, select the rules 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.

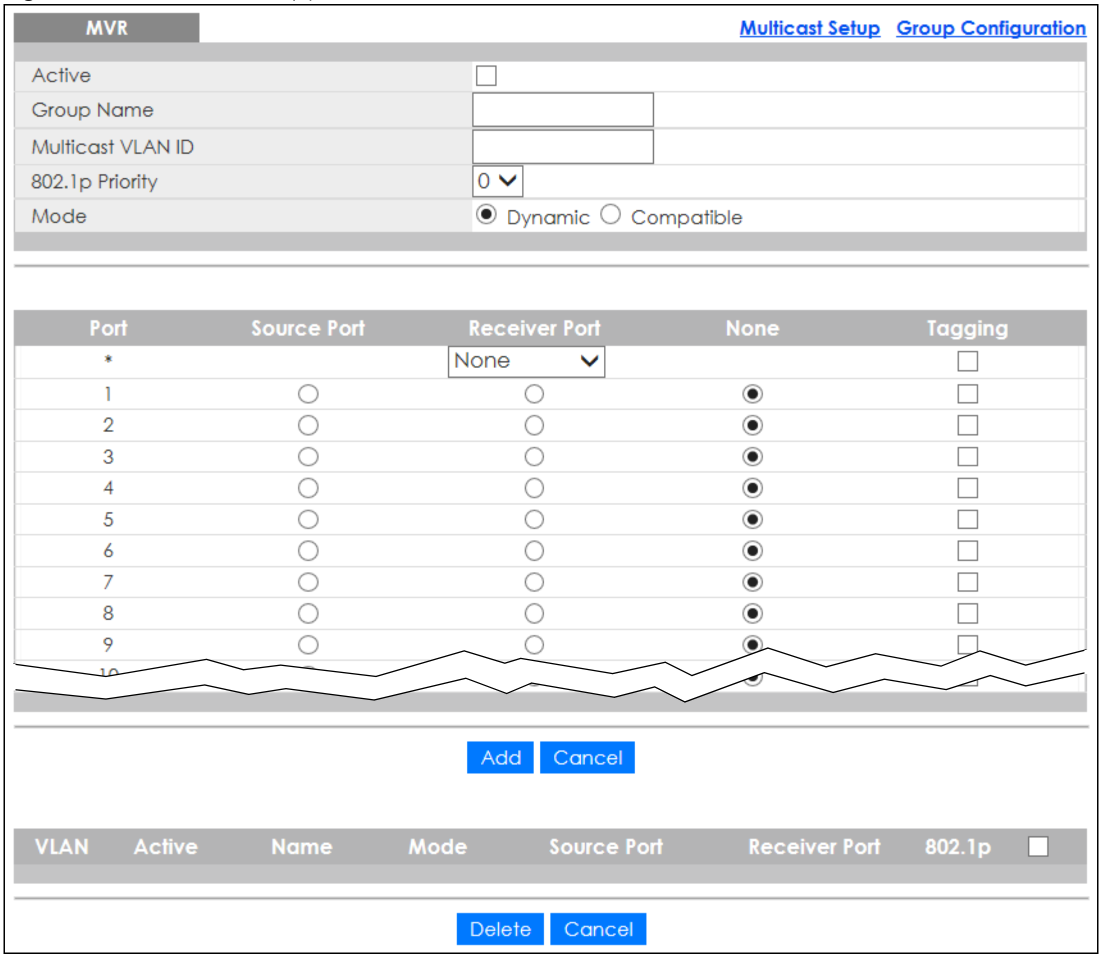
24.5 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver ports 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 183 Advanced Application > Multicast > MVR



The following table describes the related labels in this screen.

Table 107 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.
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.

Table 107   Advanced Application > Multicast > MVR (continued)

LABEL	DESCRIPTION
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 check box 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 numbers.
Receiver Port	This field displays the receiver port numbers.
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 VLANs, select the rules that you want to remove, then click the **Delete** button.
Cancel	Click **Cancel** to clear the check boxes.

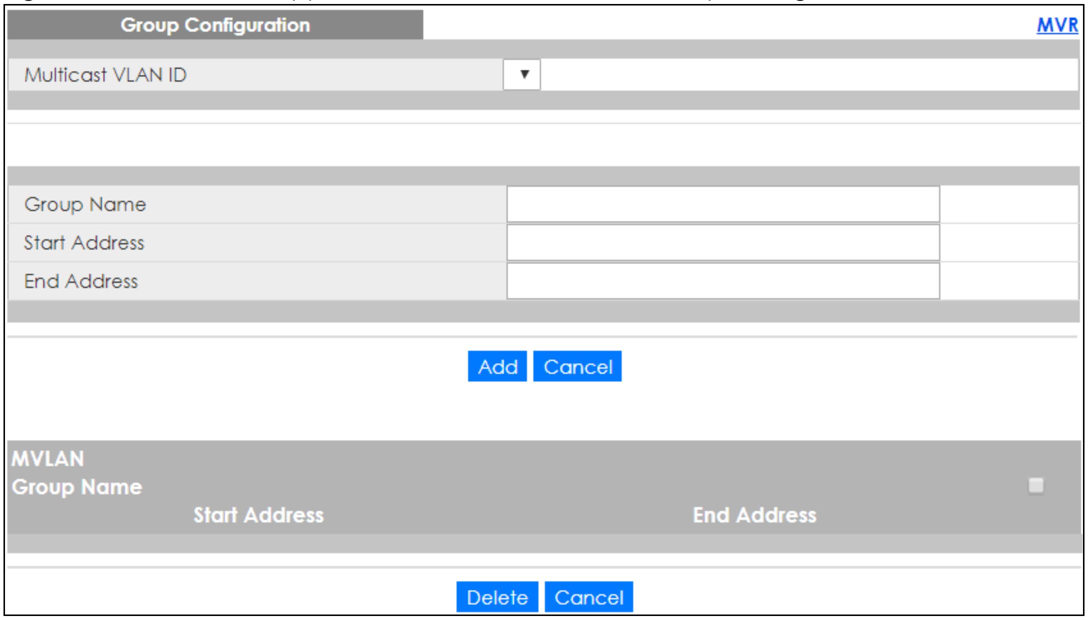
24.5.1 MVR Group Configuration

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 addresses. 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 184 Advanced Application > Multicast > MVR > Group Configuration



The following table describes the labels in this screen.

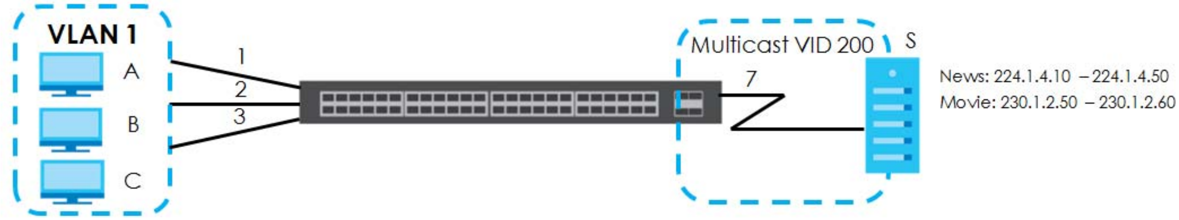
Table 108 Advanced Application > Multicast > MVR > Group Configuration

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.
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.
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.
	To delete the profiles and all the accompanying rules, select the profiles 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 rules from a profile, select the rules that you want to remove, then click the **Delete** button.
Delete	Select the entries that you want to remove, then click the **Delete** button to remove the selected entries 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 check boxes in the table.

24.5.2 MVR Configuration Example

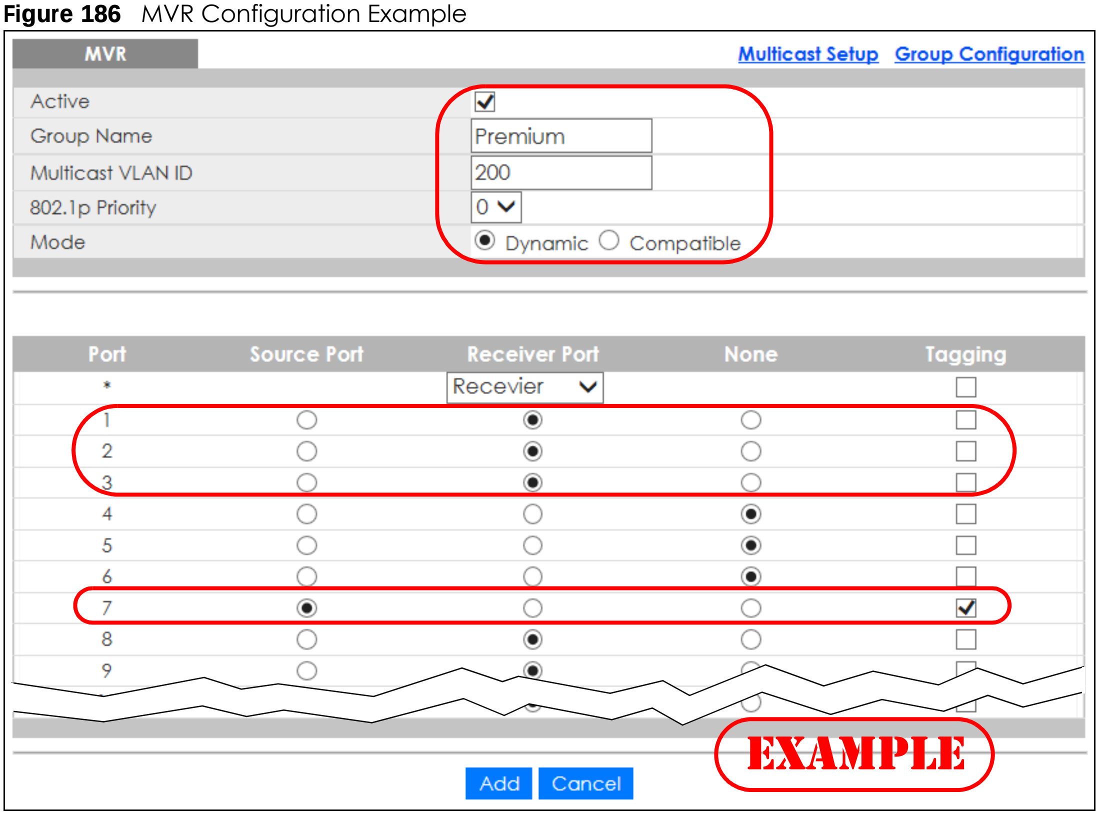
The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in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

Figure 185 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 186 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 187 MVR Group Configuration Example-1

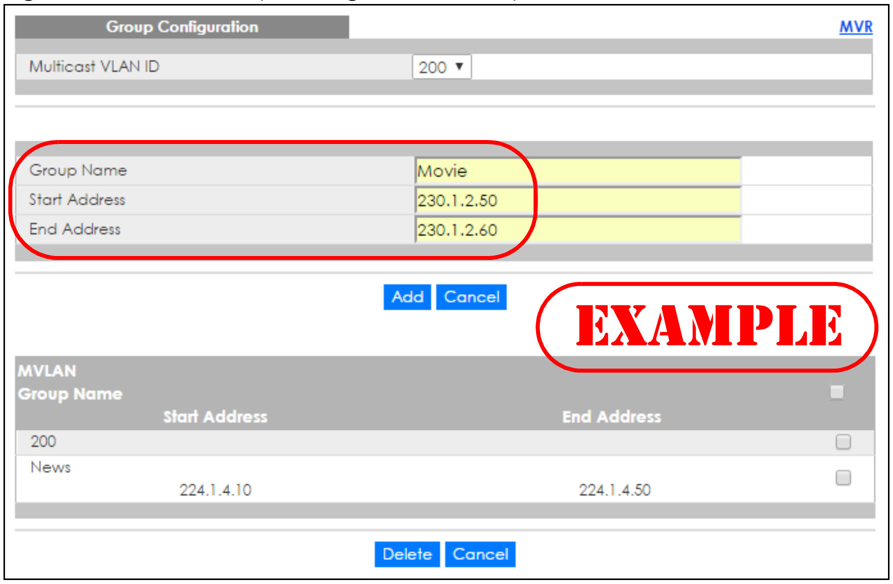
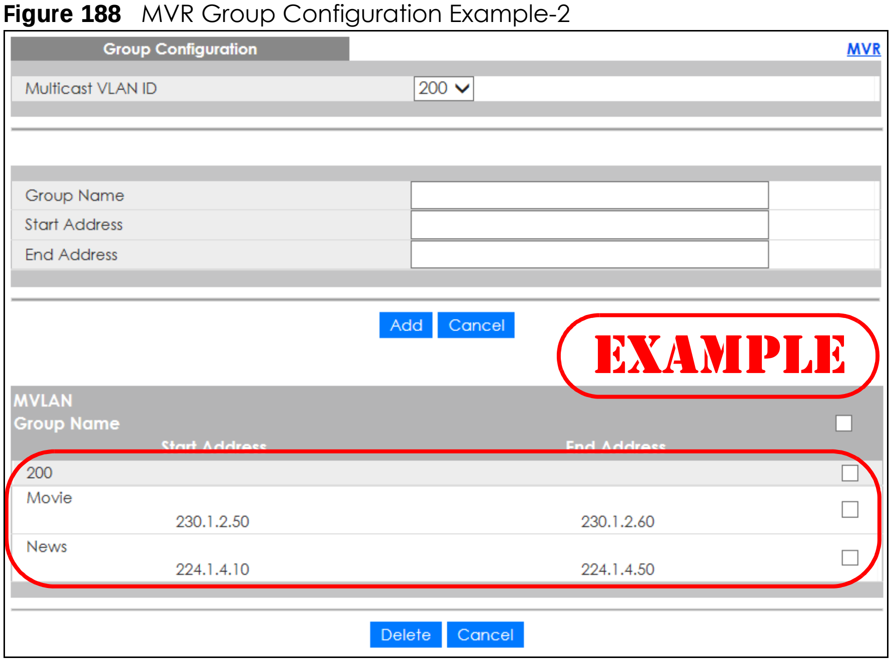


Figure 188 MVR Group Configuration Example-2



CHAPTER 25
AAA

25.1 Authentication, Authorization and Accounting (AAA)

This chapter describes how to configure authentication, authorization and accounting settings on 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) as the external authentication, authorization, and accounting server.

Figure 189 AAA Server

25.1.1 What You Can Do

- Use the **AAA** screen (Section 25.2 on page 249) to display the links to the screens where you can enable authentication and authorization or both of them on the Switch.
- use the **RADIUS Server Setup** screen (Section 25.3 on page 249) to configure your RADIUS server settings.
- Use the **TACACS+ Server Setup** screen (Section 25.4 on page 251) to configure your TACACS+ authentication settings.
- Use the **AAA Setup** screen (Section 25.5 on page 253) to configure authentication, authorization and accounting settings, such as the methods used to authenticate users accessing the Switch and which database the Switch should use first.

25.1.2 What You Need to Know

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.

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 Section 47.4 on page 412).

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 109 RADIUS vs. TACACS+

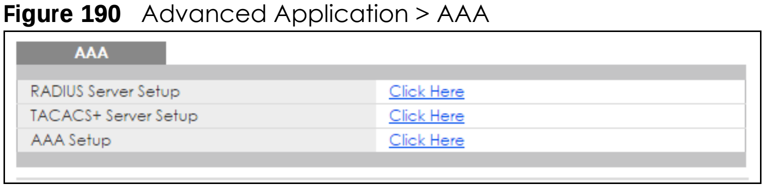
	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

25.2 AAA Screens

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

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

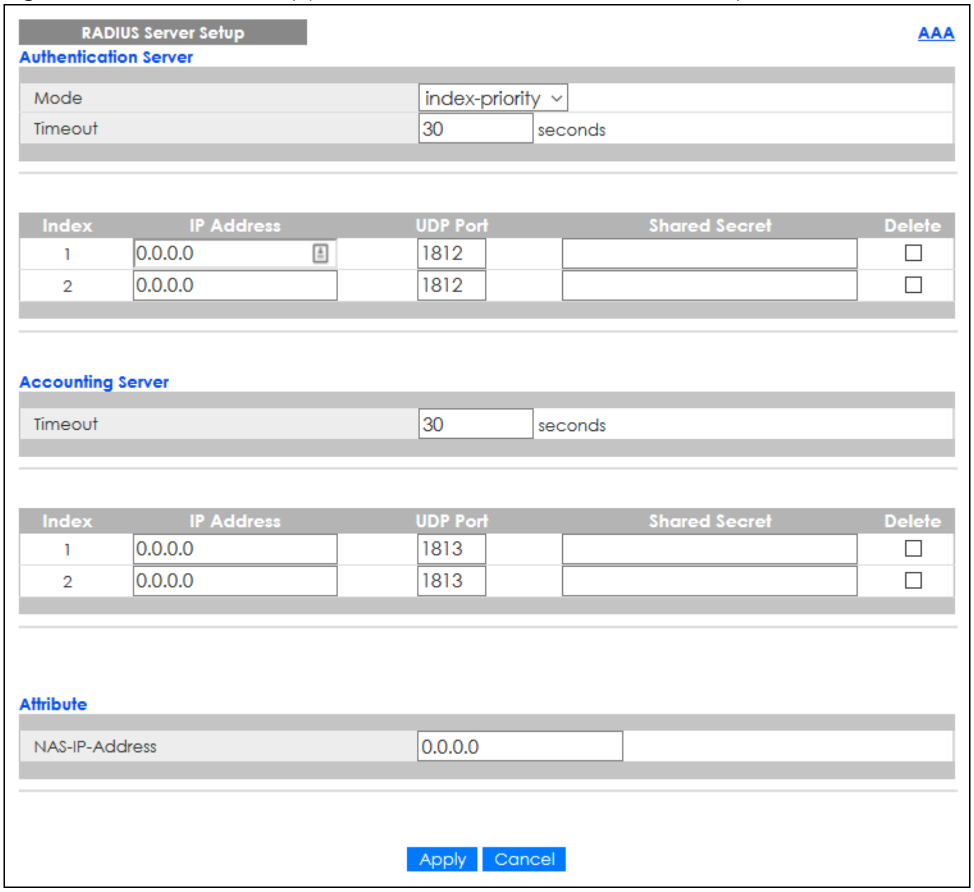
Figure 190 Advanced Application > AAA



25.3 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. Click the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 191 Advanced Application > AAA > RADIUS Server Setup



The following table describes the labels in this screen.

Table 110 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field is only valid if you configure multiple RADIUS servers. Select **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.

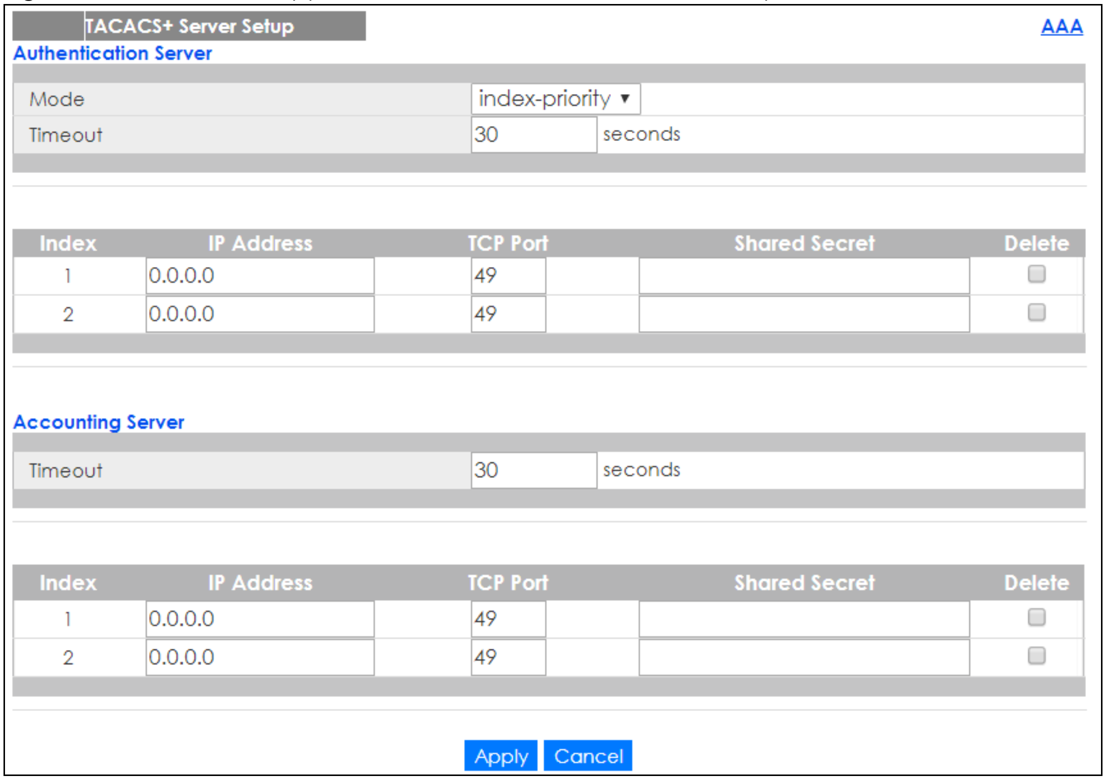
Table 110 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click **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.
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**.
Attribute	Use this section to define the RADIUS server attribute for its account.
NAS-IP-Address	Enter the IP address of the NAS (Network Access 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.

25.4 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. Click on the **TACACS+ Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 192 Advanced Application > AAA > TACACS+ Server Setup



The following table describes the labels in this screen.

Table 111 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.

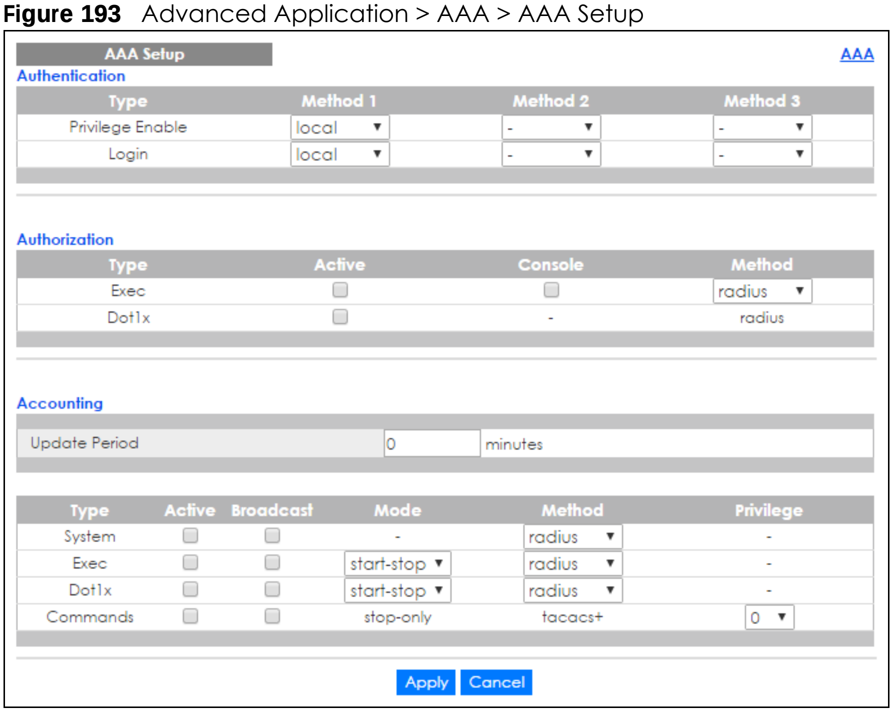
Table 111   Advanced Application > AAA > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
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.

25.5 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 193   Advanced Application > AAA > AAA Setup



The following table describes the labels in this screen.

Table 112   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.
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 into the Switch through Telnet or SSH to have a 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.

Table 112 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Type	The Switch supports the following types of events to be sent to the accounting servers: • **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 do not select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it does not get a response from the accounting server then it tries the second accounting server.
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.

25.6 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

25.6.1 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 25.5 on page 253).

Table 113 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 servers and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

25.6.1.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that these attributes only work when you enable authorization (see Section 25.5 on page 253).

Table 114 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.

25.6.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication.

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

25.6.3 Attributes Used for Authentication

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

25.6.3.1 Attributes Used for Authenticating Privilege Access

User-Name

– The format of the User-Name attribute is **$enab**#**$**, where # is the privilege level (1 – 14).

User-Password

NAS-Identifier

NAS-IP-Address

25.6.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

25.6.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

– This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

25.6.4 Attributes Used for Accounting

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

25.6.4.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID
- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 2007041917210300000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

25.6.4.2 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 115 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 116 RADIUS Attributes – Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-IP-Address	✔	✔	✔

Table 116 RADIUS Attributes – Exec Events via Telnet/SSH (continued)

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Service-Type	✔	✔	✔
Calling-Station-Id	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Session-Time		✔	✔
Acct-Terminate-Cause			✔

25.6.4.3 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 117 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		✔	✔

CHAPTER 26
IP Source Guard

26.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

26.1.1 What You Can Do

- Use the **IP Source Guard** screen (Section 26.2 on page 262) to look at the current bindings for DHCP snooping and ARP inspection.
- Use the **IP Source Guard Static Binding** screen (Section 26.4 on page 263) to manage static bindings for DHCP snooping and ARP inspection.
- Use the **DHCP Snooping** screen (Section 27.2 on page 266) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Configure** screen (Section 27.3 on page 269) 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 27.3.1 on page 270) to specify whether ports are trusted or untrusted ports for DHCP snooping.

- Use the **DHCP Snooping VLAN Configure** screen (Section 27.3.2 on page 271) 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 27.3.3 on page 272) to apply a different DHCP option 82 profile to certain ports in a VLAN.
- Use the **ARP Inspection Status** screen (Section 28.1 on page 276) 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 28.1.1 on page 277) to look at various statistics about ARP packets in each VLAN.
- Use the **ARP Inspection Log Status** screen (Section 28.1.2 on page 277) 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 28.2 on page 278) 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 28.2.1 on page 280) to specify whether ports are trusted or untrusted ports for ARP inspection.
- Use the **ARP Inspection VLAN Configure** screen (Section 28.2.2 on page 281) 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 28.4 on page 282) 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 28.5 on page 283) 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 28.6 on page 285) 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 28.7 on page 286) 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 28.8 on page 286) 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 28.9 on page 287) to enable a DHCPv6 snooping policy on a specific VLAN interface.
- Use the **Advanced Application** > **IP Source Guard** > **IPv6 DHCP Trust Setup** screen (Section 28.10 on page 288) to specify which ports are trusted and untrusted for DHCP snooping.

26.1.2 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:

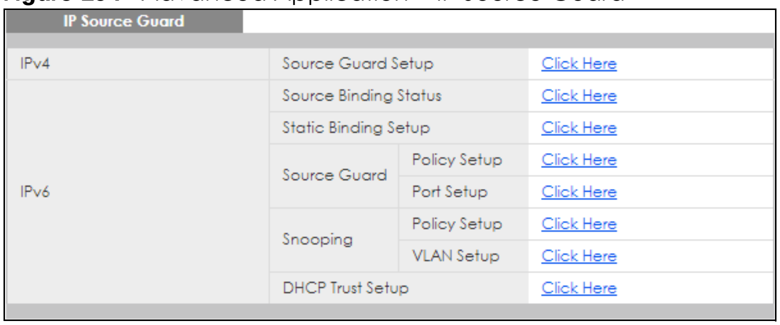
- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

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.

26.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application** > **IP Source Guard**.

Figure 194 Advanced Application > IP Source Guard



The following table describes the labels in this screen.

Table 118 Advanced Application > IP Source Guard

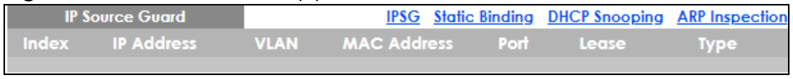
LABEL	DESCRIPTION
IPv4 Source Guard Setup	Click the link to open screens where you can view and manage static bindings, configure DHCP snooping or ARP inspection and look at various statistics.
IPv6 Source Binding Status	Click the link to open a screen where you can view the current IPv6 dynamic and static bindings or remove dynamic bindings based on IPv6 address and/or IPv6 prefix.
IPv6 Static Binding Setup	Click the link to open a screen where you can manually create IPv6 source guard static binding entries.
IPv6 Source Guard Policy Setup	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.
IPv6 Source Guard Port Setup	Click the link to open a screen where you can apply the configured IPv6 source guard policy to a port.
IPv6 Snooping Policy Setup	Click the link to open a screen where you can set up DHCPv6 snooping policies for the binding table.
IPv6 Snooping VLAN Setup	Click the link to open a screen where you can enable a DHCPv6 snooping policy on a specific VLAN interface.
IPv6 DHCP Trust Setup	Click the link to open a screen where you can specify which ports are trusted for DHCPv6 snooping.

26.3 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 195 Advanced Application > IP Source Guard > IPv4 Source Guard Setup



The following table describes the labels in this screen.

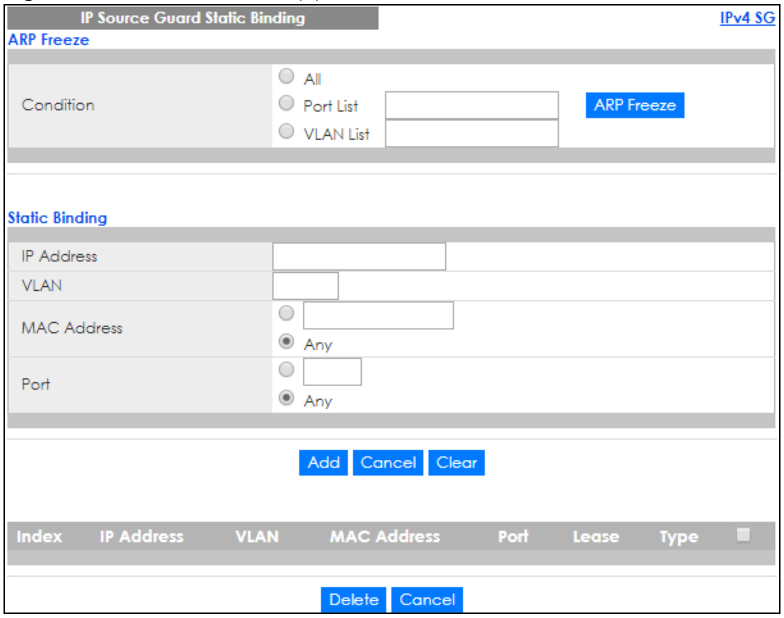
Table 119 Advanced Application > IP Source Guard > IPv4 Source Guard Setup

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
VLAN	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address 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. **static**: This binding was learned from information provided manually by an administrator. **dhcp-snooping**: This binding was learned by snooping DHCP packets.

26.4 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 196 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > Static Binding



The following table describes the labels in this screen.

Table 120 Advanced Application > 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 ports (separated by a comma). ARP entries learned on the specified ports are added to the static bindings table after you click **ARP Freeze**. **VLAN List** – Select this and enter the ID number of the VLANs (separated by a comma). ARP entries for the specified VLANs are added to the static bindings table after you click **ARP Freeze**.
Static Binding	
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
MAC Address	Enter the source MAC address in the binding. If this binding applies to all MAC addresses, select **Any**.
Port	Specify the ports 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 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.

Table 120 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > Static Binding

LABEL	DESCRIPTION
IP Address	This field displays the IP address assigned to the MAC address in the binding.
VLAN	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address in the binding.
Port	This field displays the port number.
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.
	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 entries that you want to remove, then click the **Delete** button to remove the selected entries from the table.
Cancel	Click this to clear the check boxes above.

CHAPTER 27 DHCP Snooping

27.1 DHCP Snooping Overview

With DHCP snooping, the Switch can build the binding table dynamically by snooping DHCP packets (dynamic bindings) and filter unauthorized DHCP packets in your network.

The Switch uses a binding table to distinguish between authorized and unauthorized DHCP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

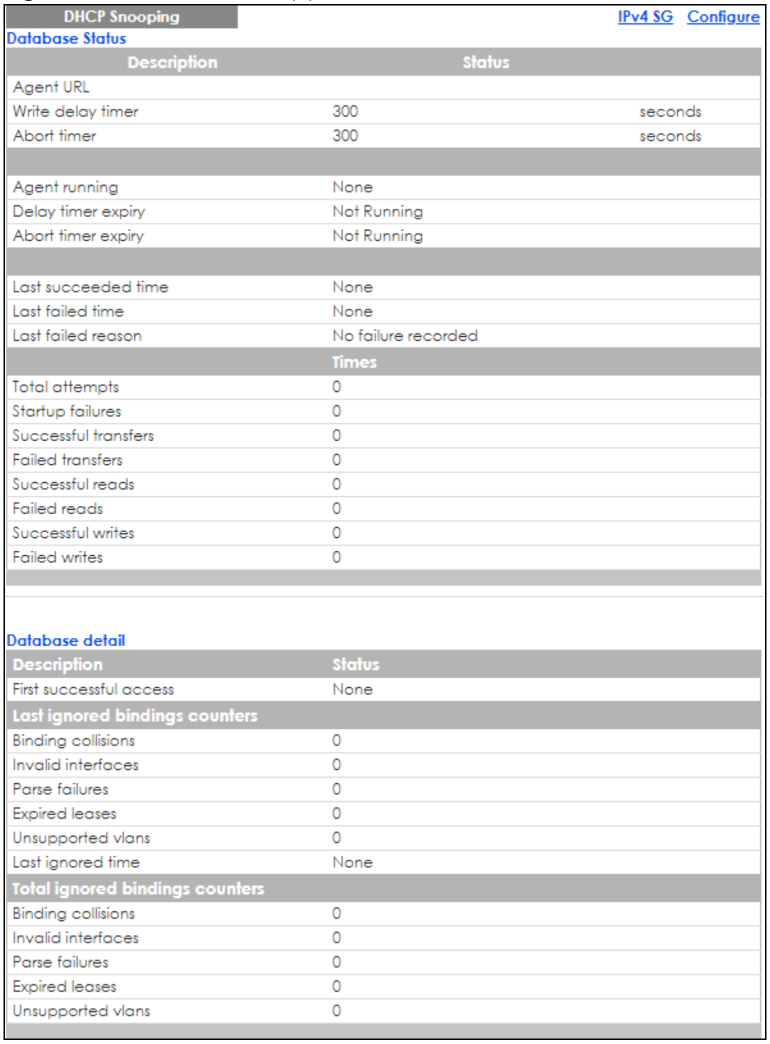
When the Switch receives a DHCP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

27.2 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 197 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping



The following table describes the labels in this screen.

Table 121 Advanced Application > 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.
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.

Table 121 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping

LABEL	DESCRIPTION
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.
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.

Table 121 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping

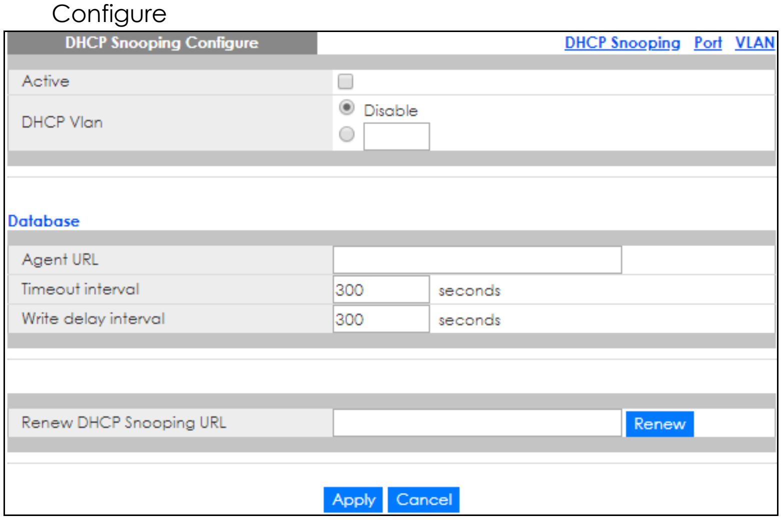
LABEL	DESCRIPTION
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays 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.

27.3 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 198 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure



The following table describes the labels in this screen.

Table 122 Advanced Application > 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 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.
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.
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.

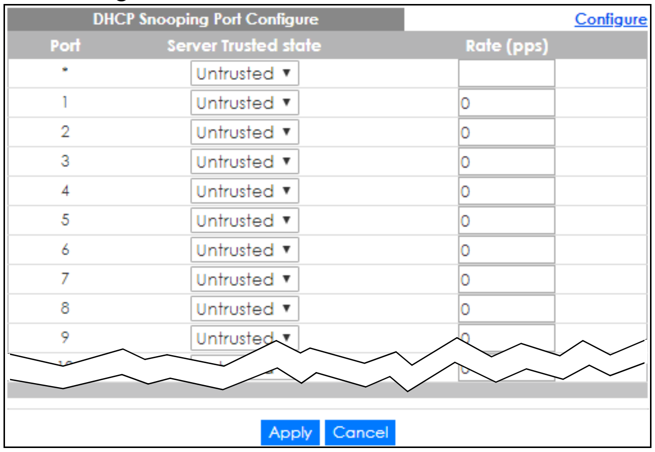
27.3.1 DHCP Snooping Port Configure

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.

Figure 199 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure> Port



The following table describes the labels in this screen.

Table 123 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port

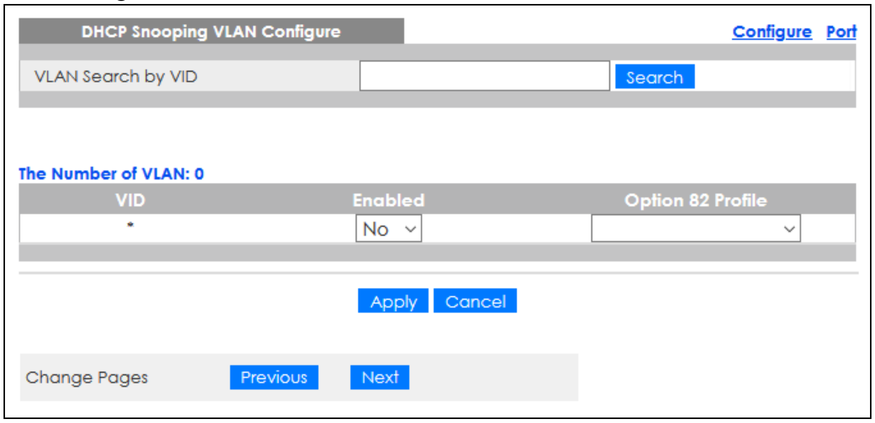
LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row 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 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.

27.3.2 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 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 200 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN



The following table describes the labels in this screen.

Table 124 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN

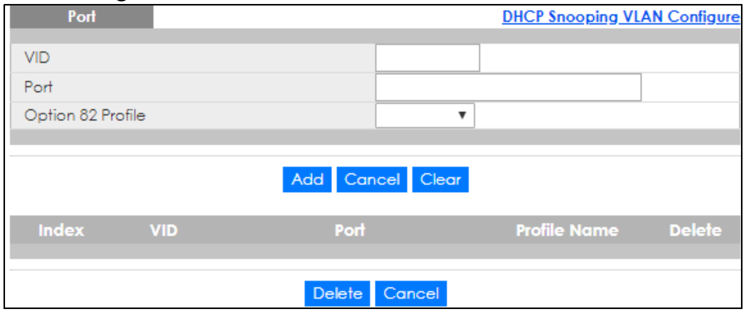
LABEL	DESCRIPTION
VLAN Search by VID	Enter the VLAN ID you want to manage. Use a comma (,) to separate individual VLANs or a dash (–) to indicates a range of VLANs. For example, “3,4” or “3–9”.
Search	Click this to display the specified range of VLANs in the section below.
VID	This field displays the 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 VLANs. 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.
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.
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

27.3.3 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 201 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN > Port



The following table describes the labels in this screen.

Table 125 Advanced Application > 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 ports 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.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports 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. 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 ports belongs.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports.
Delete	Select the entries that you want to remove in the **Delete** column, and then click the **Delete** button to remove the selected entries from the table.
Cancel	Click this to clear the **Delete** check boxes above.

27.4 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

27.4.1 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.

27.4.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

27.4.1.2 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 202 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.

27.4.1.3 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.

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.

27.4.1.4 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

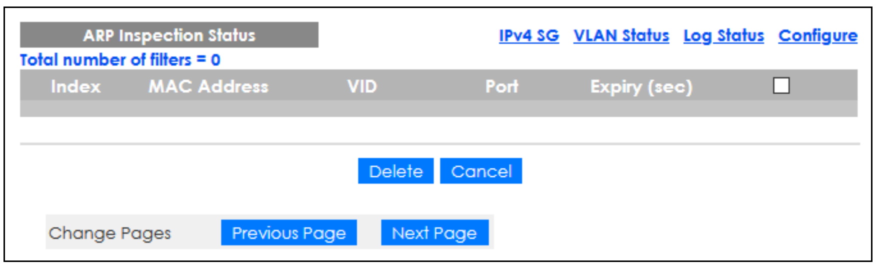
1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.
3. Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
4. Configure static bindings.

CHAPTER 28
ARP Inspection

28.1 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 203 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection Status



The following table describes the labels in this screen.

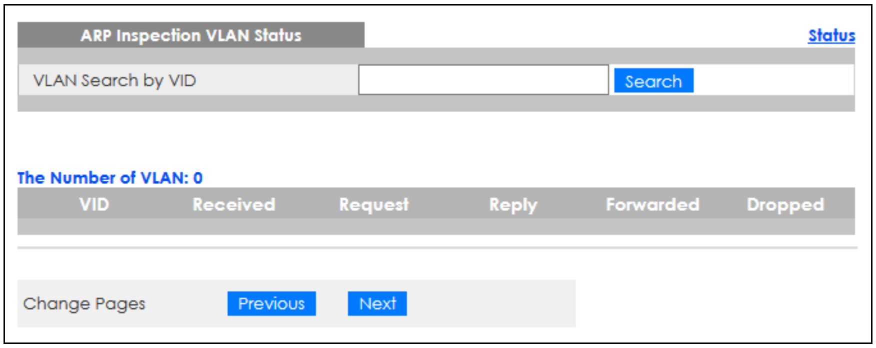
Table 126 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection Status

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.
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**).
	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 Page** or **Next Page** to show the previous or next screen if all status information cannot be seen in one screen.

28.1.1 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 204 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > VLAN Status



The following table describes the labels in this screen.

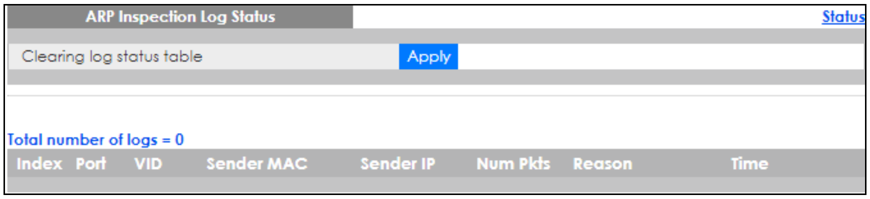
Table 127 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Use a comma (,) to separate individual VLANs or a dash (–) to indicates a range of VLANs. For example, “3,4” or “3–9”.
Search	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.
Change Pages	Click **Previous Page** or **Next Page** to show the previous/next screen if all status information cannot be seen in one screen.

28.1.2 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 205 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Log Status



The following table describes the labels in this screen.

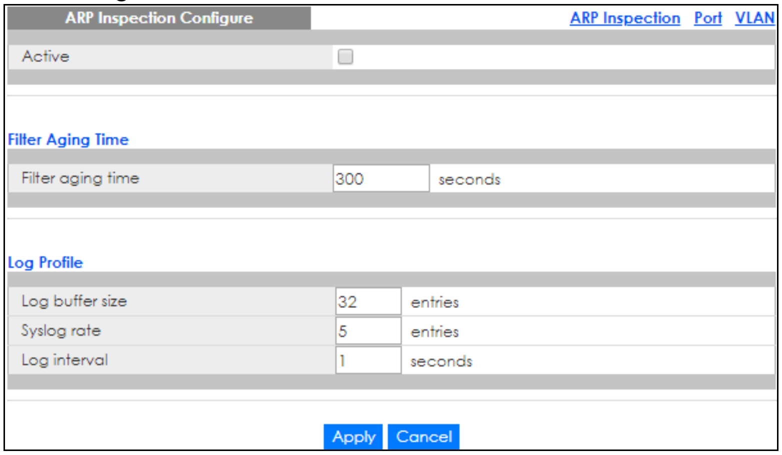
Table 128 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Log Status

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.
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.
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.
Time	This field displays when the log message was generated.

28.2 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 206 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure



The following table describes the labels in this screen.

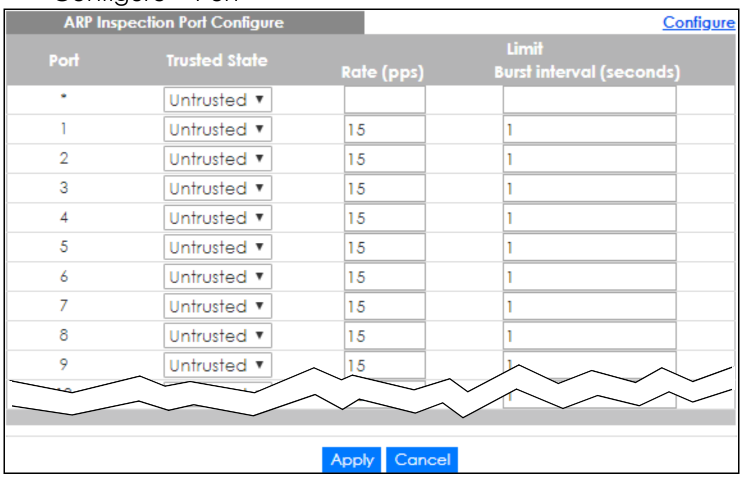
Table 129 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure

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.
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 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: • Four invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 1: the Switch sends 4 syslog messages every second. • Six 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**.
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.

28.2.1 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 207 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port



The following table describes the labels in this screen.

Table 130 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port

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

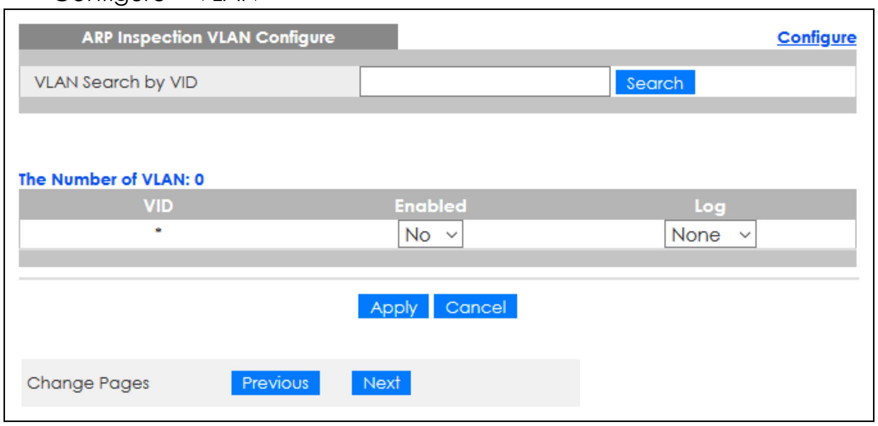
Table 130 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port (continued)

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.

28.2.2 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 208 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN



The following table describes the labels in this screen.

Table 131 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN

LABEL	DESCRIPTION
VLAN Search by VID	Specify the VLANs you want to manage in the section below. Use a comma (,) to separate individual VLANs or a dash (–) to indicates a range of VLANs. For example, "3,4" or "3–9".
Search	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.

Table 131 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN (continued)

LABEL	DESCRIPTION
Cancel	Click this to reset the values in this screen to their last-saved values.
Change Pages	Click **Previous Page** or **Next Page** to show the previous or next screen if all status information cannot be seen in one screen.

28.3 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:

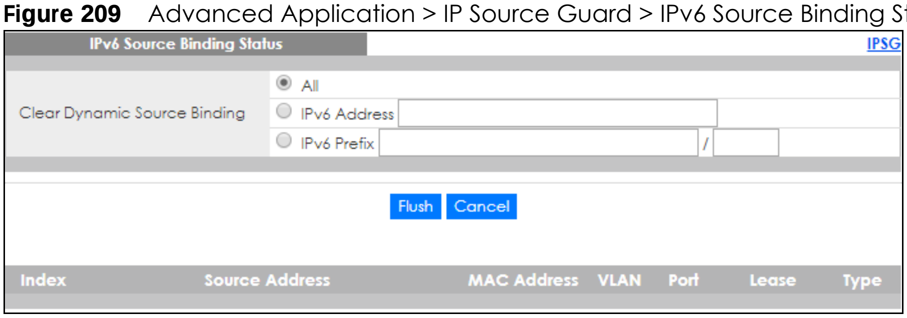
- IPv6 address
- IPv6 prefix
- VLAN ID
- Port number
- MAC address

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.

28.4 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 209 Advanced Application > IP Source Guard > IPv6 Source Binding Status



The following table describes the labels in this screen.

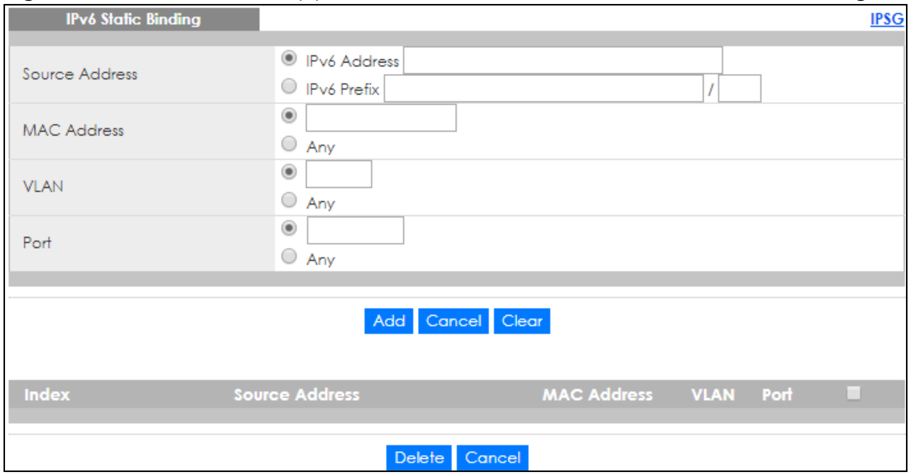
Table 132 Advanced Application > IP Source Guard > IPv6 Source Binding Status

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.

28.5 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 210 Advanced Application > IP Source Guard > IPv6 Static Binding Setup



The following table describes the labels in this screen.

Table 133 Advanced Application > IP Source Guard > IPv6 Static Binding Setup

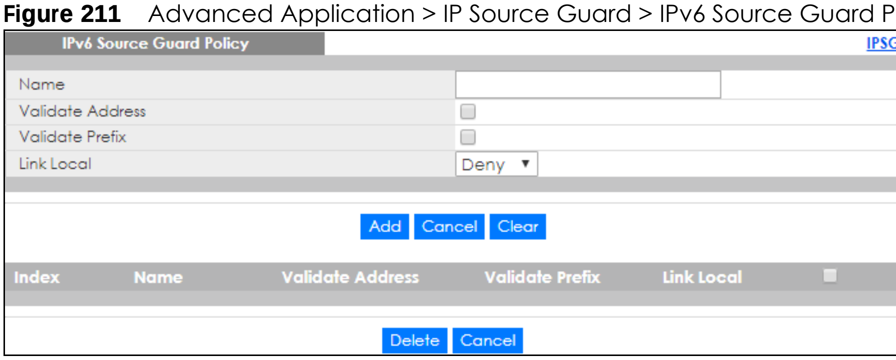
LABEL	DESCRIPTION
IPv6 Static Binding	
Source Address	Enter the IPv6 address or IPv6 prefix and prefix length in the binding.
MAC Address	Enter the source MAC address in the binding. If this binding does not check this field, select **Any**. Note: You cannot choose **Any** for all three of **MAC Address**, **VLAN** and **Port**. You must fill in at least one.
VLAN	Enter the source VLAN ID in the binding. If this binding does not check this field, select **Any**.
Port	Specify the ports 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.
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.
	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 check box and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

28.6 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 211 Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup



The following table describes the labels in this screen.

Table 134 Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup

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.
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.
	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.

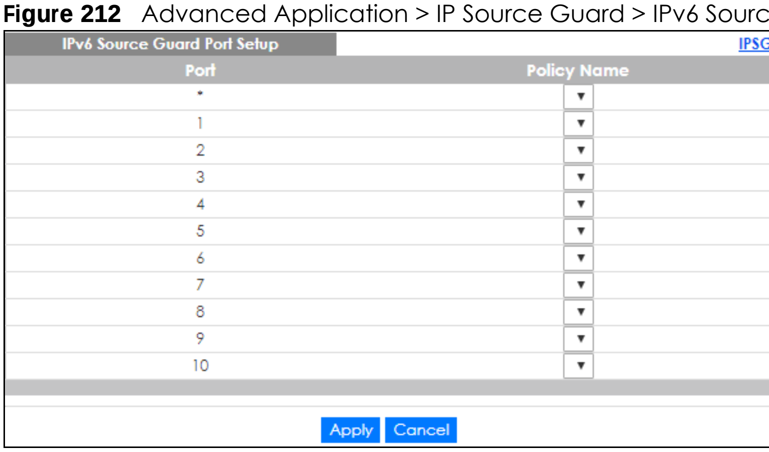
Table 134   Advanced Application > IP Source Guard > IPv6 Source Guard Policy Setup

LABEL	DESCRIPTION
Delete	Select an entry check box and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

28.7 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 212   Advanced Application > IP Source Guard > IPv6 Source Guard Port Setup



The following table describes the labels in this screen.

Table 135   Advanced Application > IP Source Guard > IPv6 Source Guard Port Setup

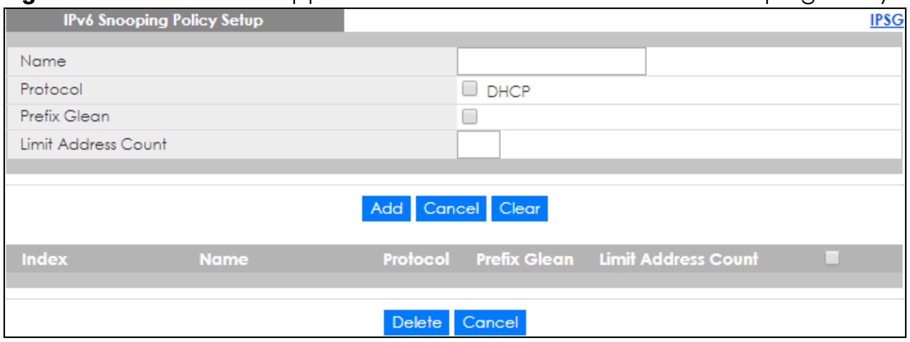
LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Policy Name	Select an IPv6 source guard policy that the Switch will apply 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 this to reset the values in this screen to their last-saved values.

28.8 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 213 Advanced Application > IP Source Guard > IPv6 Snooping Policy Setup



The following table describes the labels in this screen.

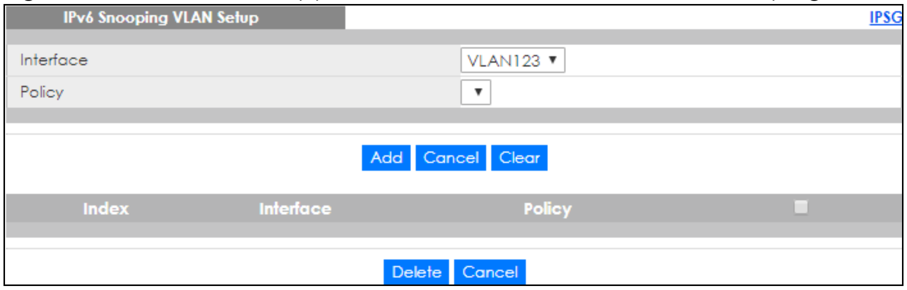
Table 136 Advanced Application > IP Source Guard > IPv6 Snooping Policy Setup

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. 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.
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 number of IPv6 addresses and prefixes learned using the IPv6 snooping policy.
Delete	Select an entry check box and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

28.9 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 214 Advanced Application > IP Source Guard > IPv6 Snooping VLAN Setup



The following table describes the labels in this screen.

Table 137 Advanced Application > IP Source Guard > IPv6 Snooping VLAN Setup

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.
	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 check box and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

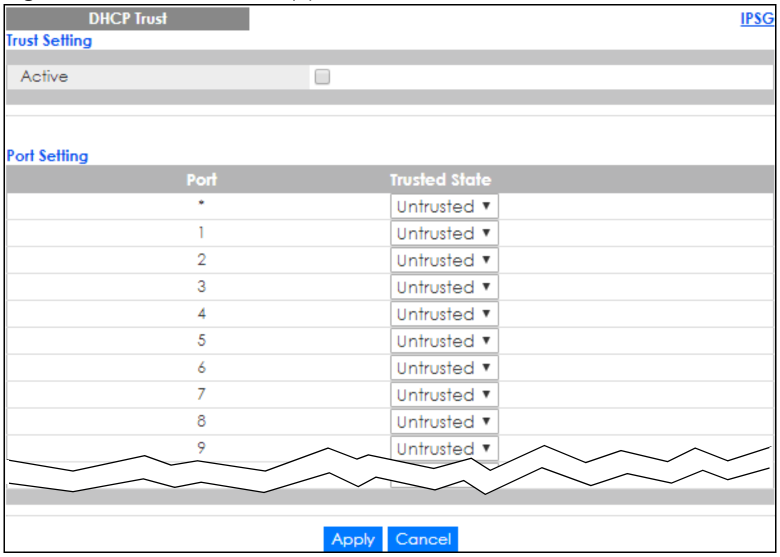
28.10 IPv6 DHCP Trust Setup

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 215 Advanced Application > IP Source Guard > IPv6 DHCP Trust Setup



The following table describes the labels in this screen.

Table 138 Advanced Application > IP Source Guard > IPv6 DHCP Trust Setup

LABEL	DESCRIPTION
Trust Setting	
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 Setting	
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
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.

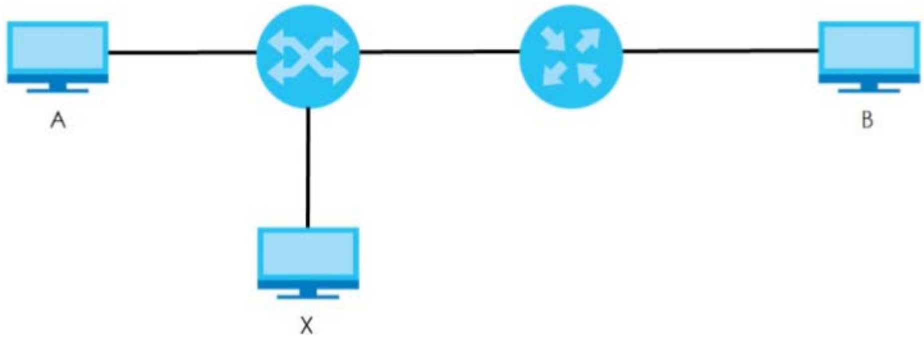
28.11 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

28.11.1 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 216 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.

28.11.1.1 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.

- 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.

28.11.1.2 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 or 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.

28.11.1.3 Syslog

The Switch can send syslog messages to the specified syslog server 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.

28.11.1.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1 Configure DHCP snooping. See Section 28.11.1 on page 290.

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.

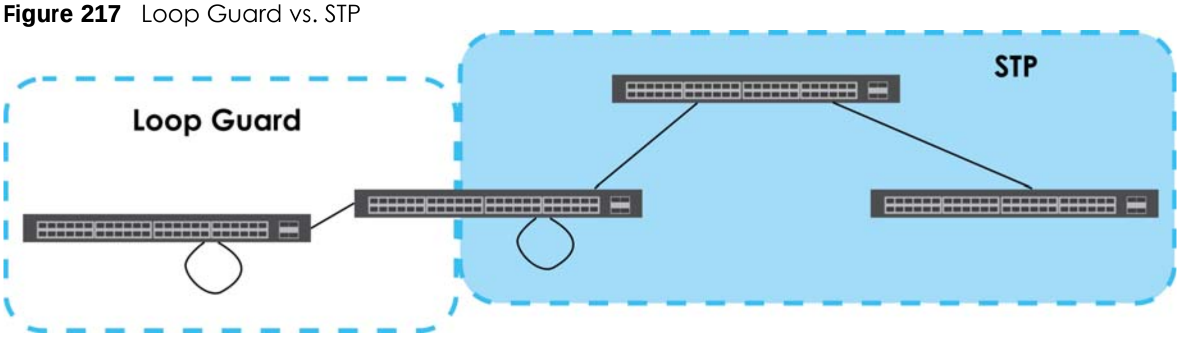
CHAPTER 29
Loop Guard

29.1 Loop Guard Overview

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

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 217 Loop Guard vs. STP



Refer to Section 29.1.2 on page 292 for more information.

29.1.1 What You Can Do

Use the **Loop Guard** screen (Section 29.2 on page 294) to enable loop guard on the Switch and in specific ports.

29.1.2 What You Need to Know

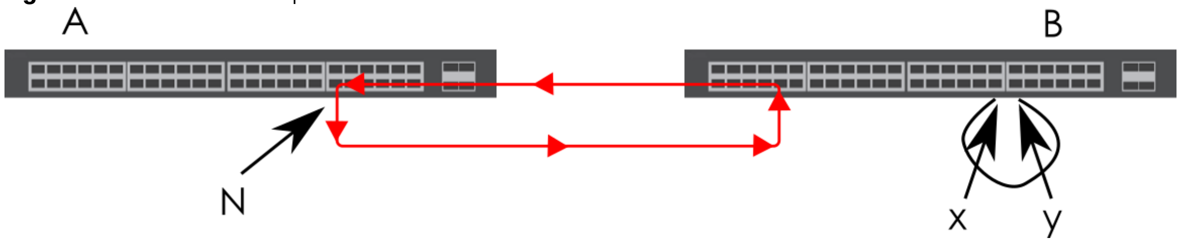
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends 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:

- The switch (not in loop state) will receive broadcast messages sent out from the switch in loop state.
- The switch (not in loop state) 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** has two ports, **x** and **y**, mistakenly connected to each other. It forms a loop. 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**.

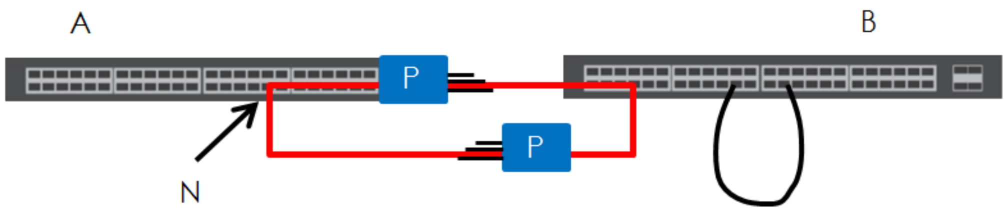
Figure 218 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a Switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

Loop guard can be enabled on both Ethernet ports. 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.

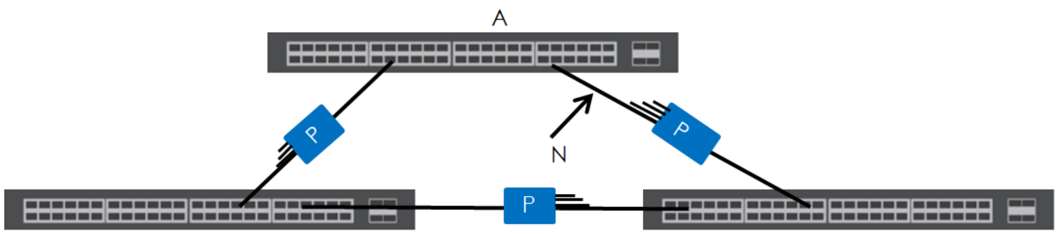
Figure 219 Loop Guard – Probe Packet



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 220 Loop Guard – Network Loop



Note: After resolving the loop problem on your network you can re-activate the disabled port via the Web Configurator (see Section 8.7 on page 111) or via commands (See the CLI Reference Guide).

29.2 Loop Guard Setup

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

Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTO or MSTP) enabled.

Figure 221 Advanced Application > Loop Guard

The following table describes the labels in this screen.

Table 139 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.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The Switch sends broadcast and multicast 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.

CHAPTER 30
VLAN Mapping

This chapter shows you how to configure VLAN mapping on the Switch.

30.1 VLAN Mapping Overview

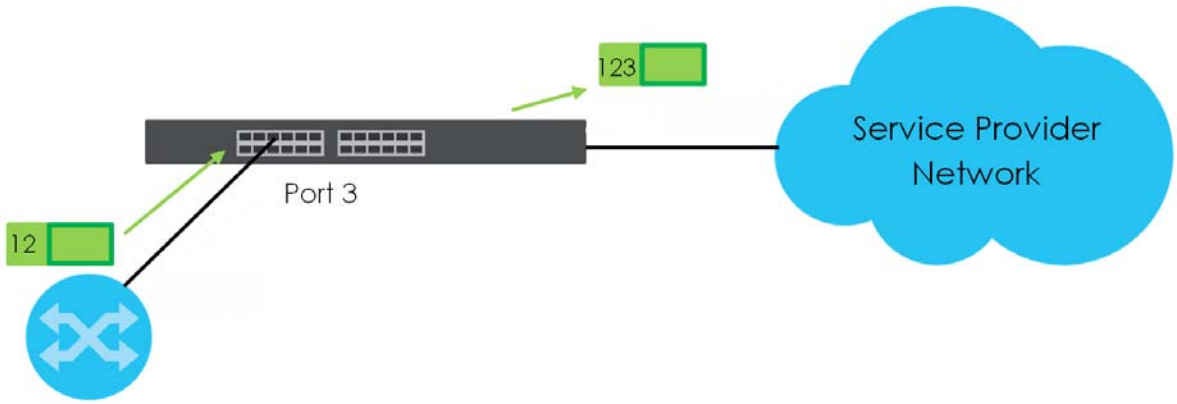
With VLAN mapping enabled, the Switch can map the VLAN ID and priority level of packets received from a private network to those used in the service provider's network.

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. If the incoming packets are untagged or tagged but do not match an entry in the VLAN mapping table, the Switch does not translate the existing VLAN ID and uses the MAC table and/or VLAN table to decide how to forward the packets.

30.1.1 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.

Figure 222 VLAN Mapping Example



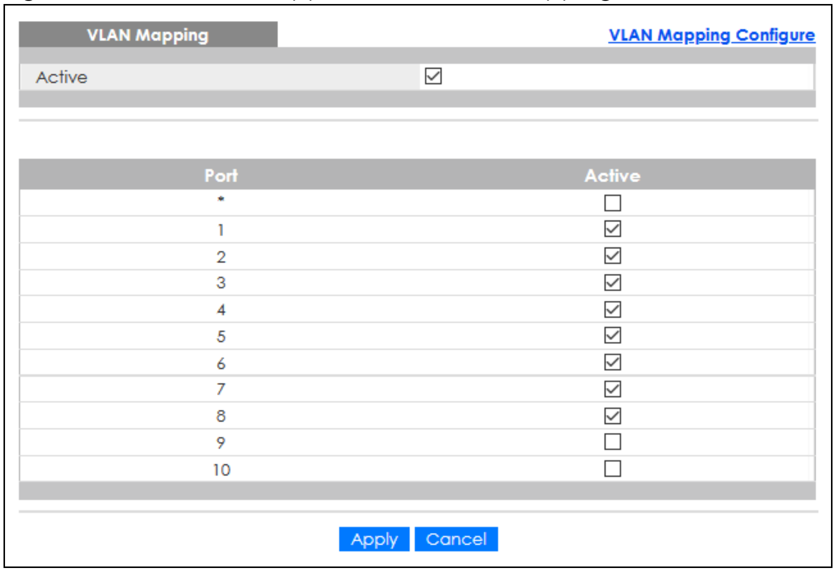
30.1.2 What You Can Do

- Use the **VLAN Mapping** screen (Section 30.2 on page 296) to enable VLAN mapping on the Switch and ports.
- Use the **VLAN Mapping Configure** screen (Section 30.2.1 on page 296) to enable and edit the VLAN mapping rules.

30.2 Enable VLAN Mapping

Click **Advanced Application** and then **VLAN Mapping** in the navigation panel to display the screen as shown.

Figure 223 Advanced Application > VLAN Mapping



The following table describes the labels in this screen.

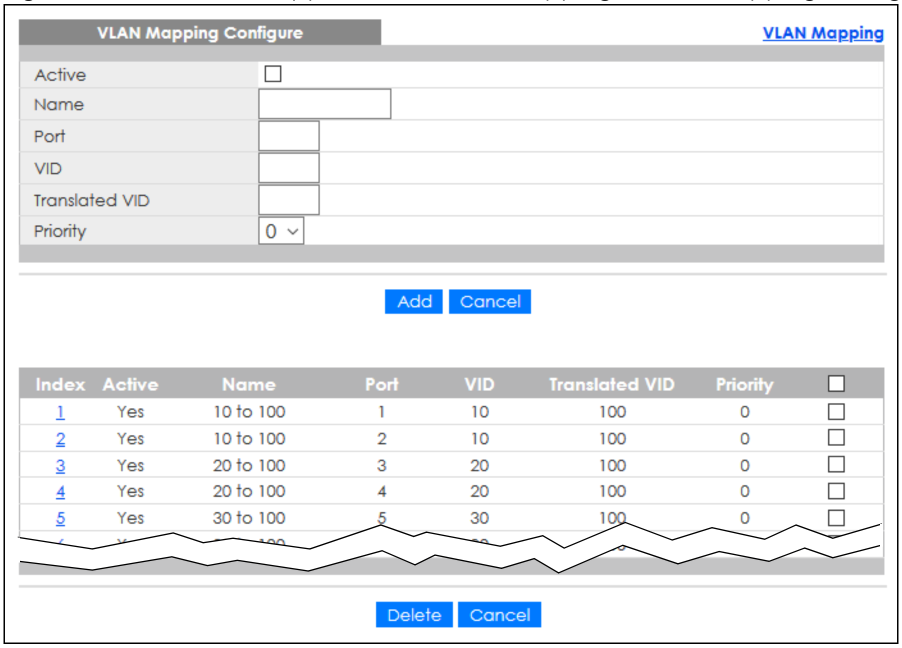
Table 140 Advanced Application > VLAN Mapping

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

30.2.1 VLAN Mapping Configure

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 rules.

Figure 224 Advanced Application > VLAN Mapping > VLAN Mapping Configuration



The following table describes the labels in this screen.

Table 141 Advanced Application > VLAN Mapping > VLAN Mapping Configuration

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	Type a port to be included in this rule.
VID	Enter a VLAN ID from 1 to 4094. This is the VLAN tag carried in the packets and will be translated into the VID you specified in the **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.
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.
	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 141 Advanced Application > VLAN Mapping > VLAN Mapping Configuration (continued)

LABEL	DESCRIPTION
Delete	Check the rules that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

CHAPTER 31
Layer 2 Protocol Tunneling

31.1 Layer 2 Protocol Tunneling Overview

This chapter shows you how to configure layer 2 protocol tunneling on the Switch.

31.1.1 What You Can Do

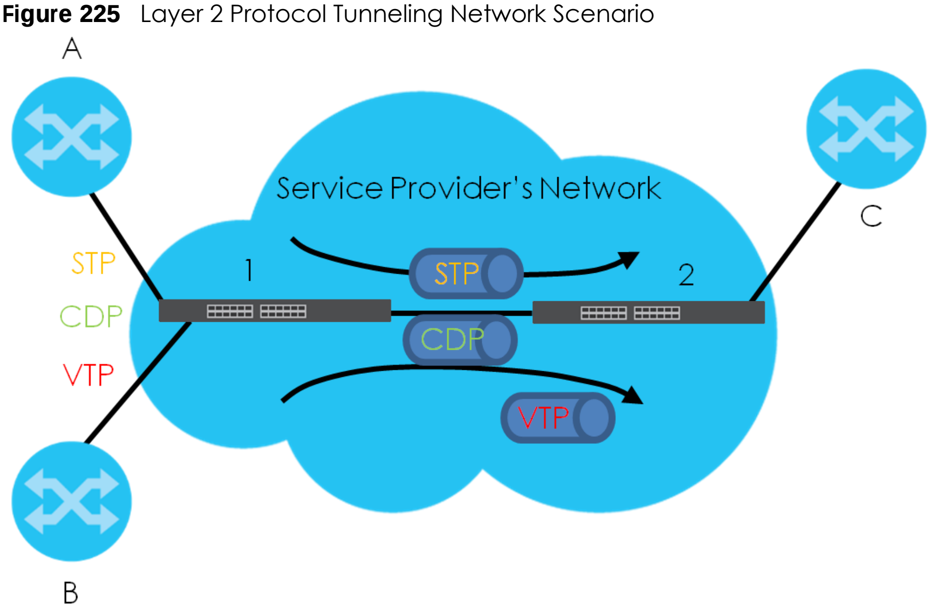
Use the **Layer 2 Protocol Tunnel** screen (Section 31.2 on page 300) to enable layer 2 protocol tunneling on the Switch and specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets.

31.1.2 What You Need to Know

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.

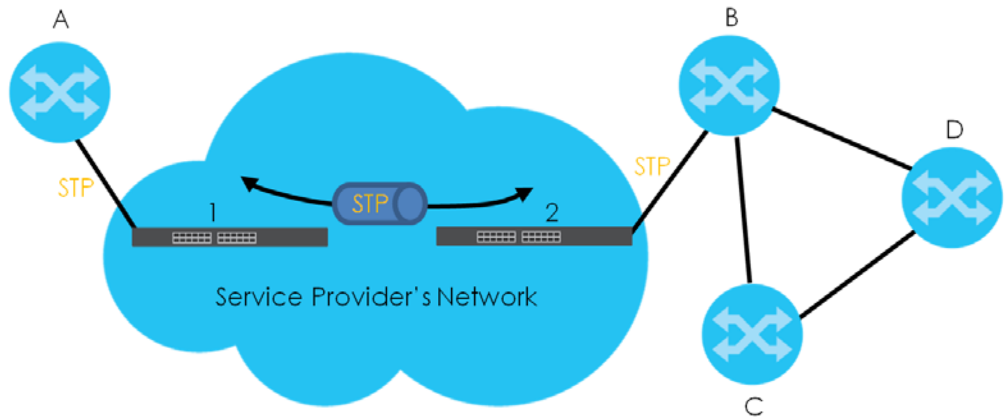
Figure 225 Layer 2 Protocol Tunneling Network Scenario



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 (Uni-Directional Link Detection).

Figure 226 L2PT Network Example



31.1.2.1 Layer 2 Protocol Tunneling Mode

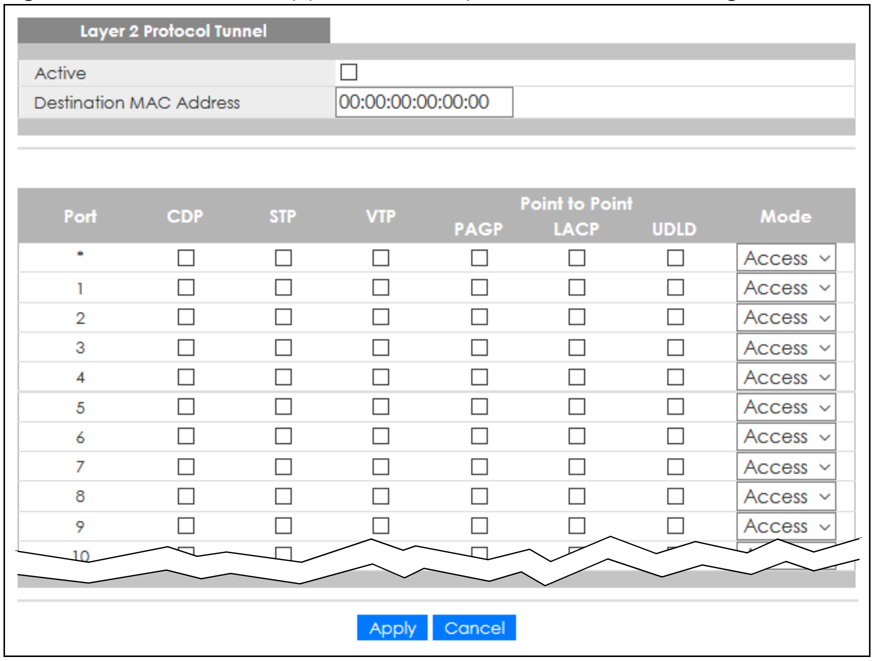
Each port can have two layer 2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in Figure 226 on page 300) 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.

31.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application** > **Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 227 Advanced Application > Layer 2 Protocol Tunneling



The following table describes the labels in this screen.

Table 142 Advanced Application > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer 2 protocol tunneling on the Switch.
Destination MAC Address	Specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number. * means all ports.
*	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.

Table 142   Advanced Application > Layer 2 Protocol Tunneling (continued)

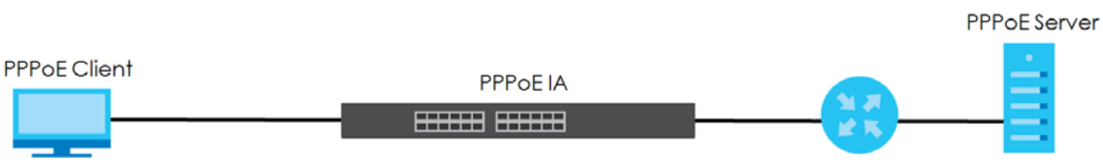
LABEL	DESCRIPTION
Point to Point	The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAgP and UDLD are Cisco's proprietary data link layer protocols. PAgP is similar to LACP 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 ports. 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 ports 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 services is not enabled on an access port, the protocol packets are dropped.
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.

CHAPTER 32
PPPoE

32.1 PPPoE Intermediate Agent Overview

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.

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.



32.1.1 What You Can Do

- Use the **PPPoE** screen (Section 32.2 on page 305) to display the main PPPoE screen.
- Use the **Intermediate Agent** screen (Section 32.3 on page 306) to enable the PPPoE Intermediate Agent on the Switch.
- Use the **PPPoE IA Per-Port** screen (Section 32.3.1 on page 307) to set the port state and configure PPPoE intermediate agent sub-options on a per-port basis.
- Use the **PPPoE IA Per-Port Per-VLAN** screen (Section 32.3.2 on page 308) to configure PPPoE IA settings that apply to a specific VLAN on a port.
- Use the **PPPoE IA for VLAN** (Section 32.3.3 on page 309) to enable the PPPoE Intermediate Agent on a VLAN.

32.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

32.1.2.1 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 143 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the "ADSL Forum" IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.

32.1.2.2 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 144 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 145 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.

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 146 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)

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 147 PPPoE IA Circuit ID Sub-option Format: Defined in WT-101

SubOpt	Length	Value								
0x01 (1 byte)	N (1 byte)	Access Node Identifier (20 byte)	Space (1 byte)	eth (3 byte)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port No (2 byte)	: (1 byte)	VLAN ID (4 bytes)

32.1.2.3 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 or 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 ports.

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 ports.
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

32.2 PPPoE

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.

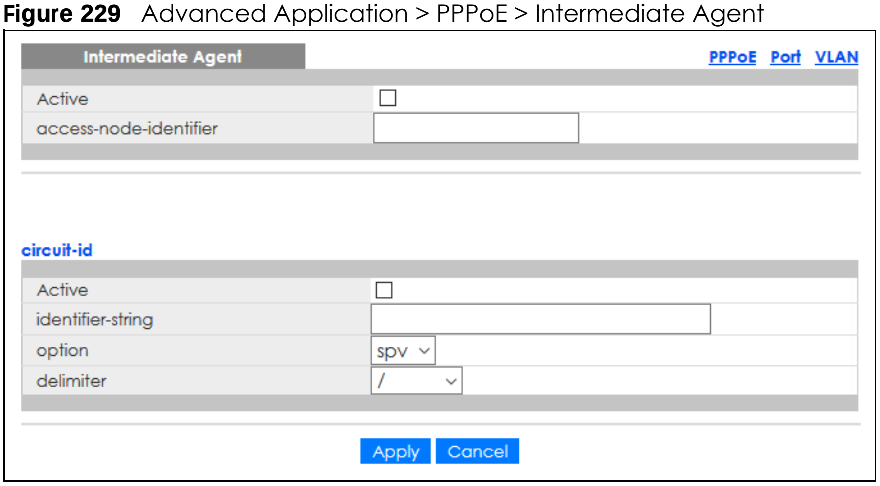
Figure 228 Advanced Application > PPPoE > Intermediate Agent

32.3 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 229 Advanced Application > PPPoE > Intermediate Agent



The following table describes the labels in this screen.

Table 148 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.

Table 148 Advanced Application > PPPoE > Intermediate Agent (continued)

LABEL	DESCRIPTION
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.

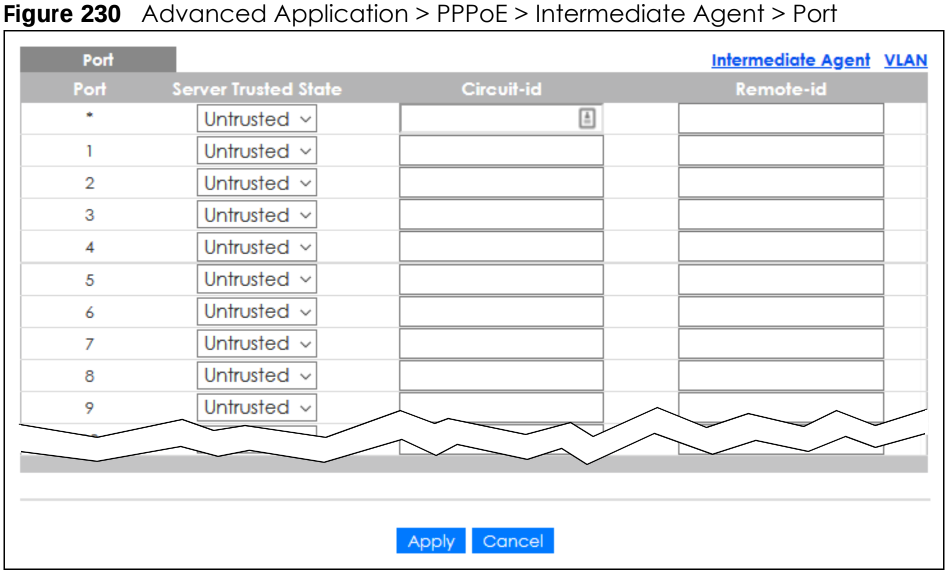
32.3.1 PPPoE IA Per-Port

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 230 Advanced Application > PPPoE > Intermediate Agent > Port



The following table describes the labels in this screen.

Table 149 Advanced Application > PPPoE > Intermediate Agent > Port

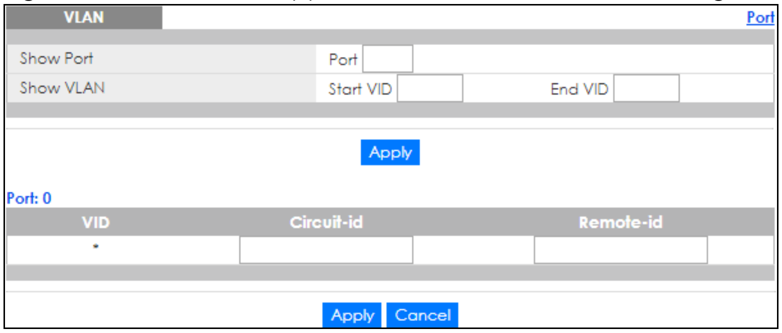
LABEL	DESCRIPTION
Port	This field displays the port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Server Trusted State	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 ports. 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 ports. 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.
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.

32.3.2 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



The following table describes the labels in this screen.

Table 150 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

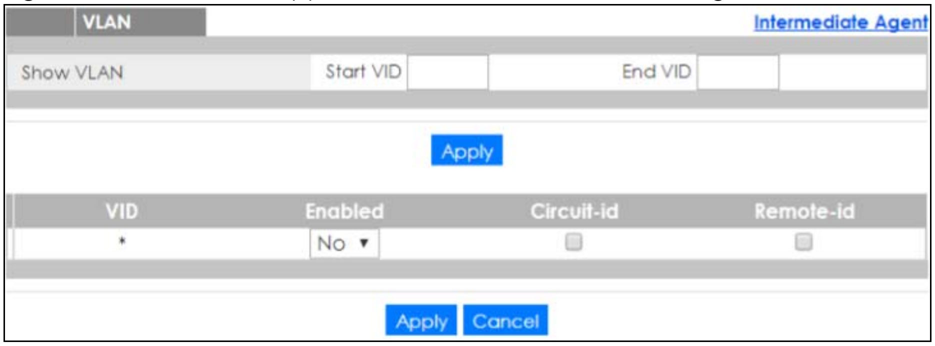
LABEL	DESCRIPTION
Show Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLAN(s) on the port.
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
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.
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. 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.

32.3.3 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 232 Advanced Application > PPPoE > Intermediate Agent > VLAN



The following table describes the labels in this screen.

Table 151 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. 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.

CHAPTER 33
Error Disable

33.1 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.

33.1.1 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 networks. You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

33.1.2 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 ports loop back to the Switch, the Switch can shut down the ports automatically. After that, you need to enable the ports or allow the packets on a port manually via the Web Configurator or the commands. With error-disable recovery, you can set the disabled ports to become active or start receiving the packets again after the time interval you specify.

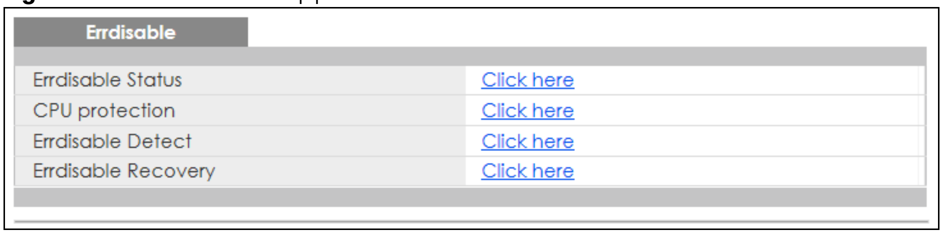
33.1.3 What You Can Do

- Use the **Errdisable Status** screen (Section 33.3 on page 312) 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 33.4 on page 314) 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 33.5 on page 315) 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 33.6 on page 316) to set the Switch to automatically undo an action after the error is gone.

33.2 Error Disable Settings

Use this screen to go to the screens where you can configure error disable related settings. Click **Advanced Application** > **Errdisable** in the navigation panel to open the following screen.

Figure 233 Advanced Application > Errdisable



The following table describes the labels in this screen.

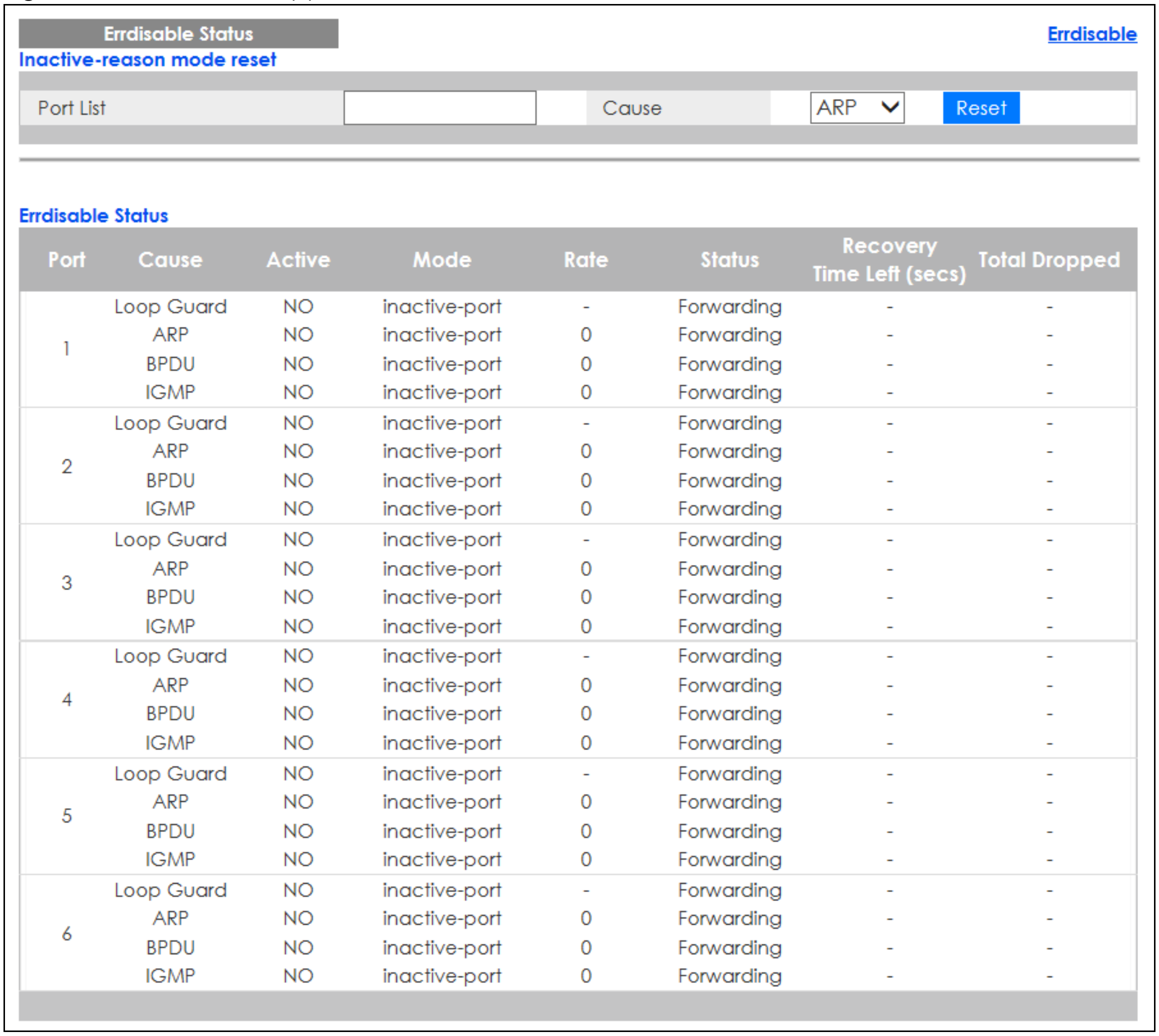
Table 152 Advanced Application > Errdisable

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.

33.3 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 234 Advanced Application > Errdisable > Errdisable Status



Port	Cause	Active	Mode	Rate	Status	Recovery Time Left (secs)	Total Dropped
1	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
2	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
3	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
4	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
5	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
6	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-

The following table describes the labels in this screen.

Table 153 Advanced Application > Errdisable > Errdisable Status

LABEL	DESCRIPTION
Inactive-reason mode reset	
Port List	Enter the number of the ports (separated by a comma) on which you want to reset inactive-reason status.
Cause	Select the cause of inactive-reason mode you want to reset here.
Reset	Press to reset the specified ports to handle ARP, BPDU or IGMP packets instead of ignoring them, if the ports is in inactive-reason mode.
Errdisable Status	
Port	This is the number of the port on which you want to configure Errdisable Status.
Cause	This displays the type of the control packet received on the port or the feature enabled on the port and causing 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.

Table 153   Advanced Application > Errdisable > Errdisable Status (continued)

LABEL	DESCRIPTION
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 ports 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 ports 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.

33.4 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 235   Advanced Application > Errdisable > CPU protection

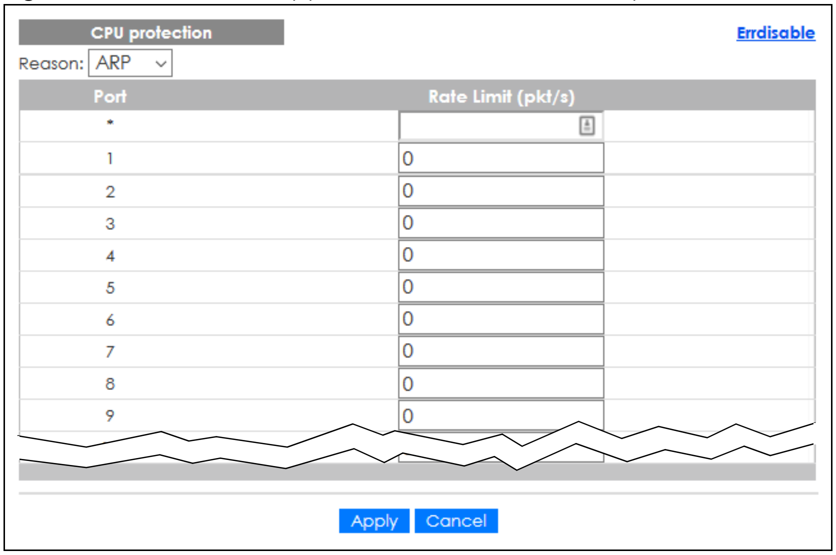
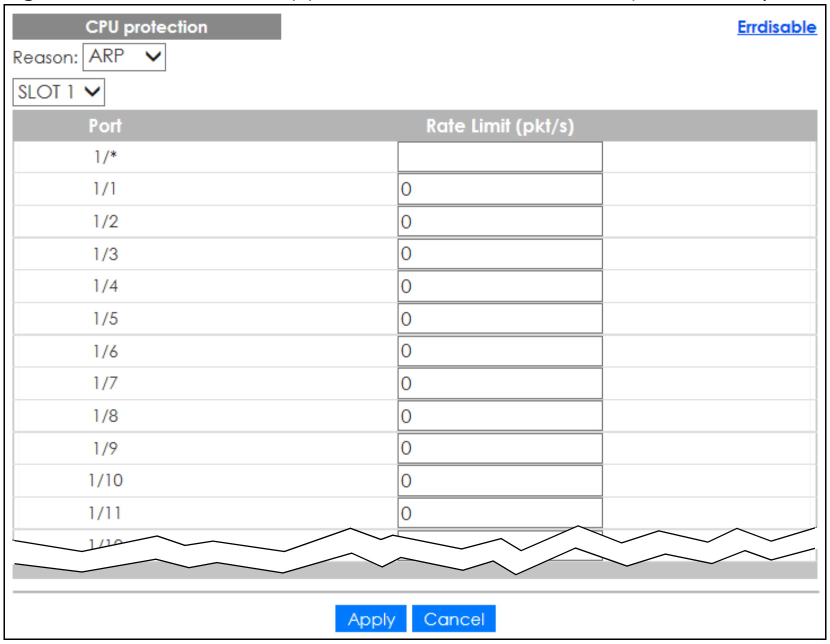


Figure 236 Advanced Application > Errdisable > CPU protection (Stacking Mode)



The following table describes the labels in this screen.

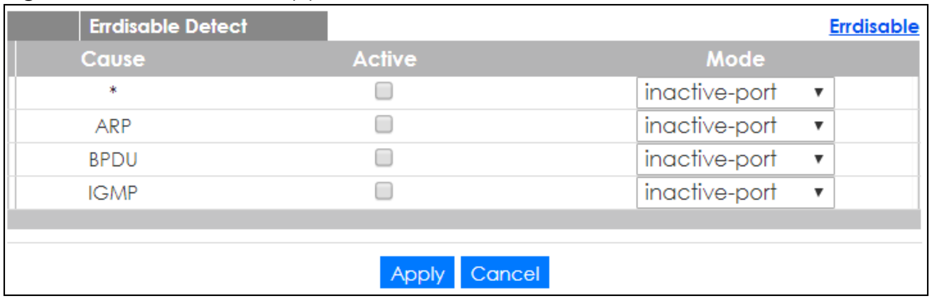
Table 154 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. 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.
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.

33.5 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 237 Advanced Application > Errdisable > Errdisable Detect



The following table describes the labels in this screen.

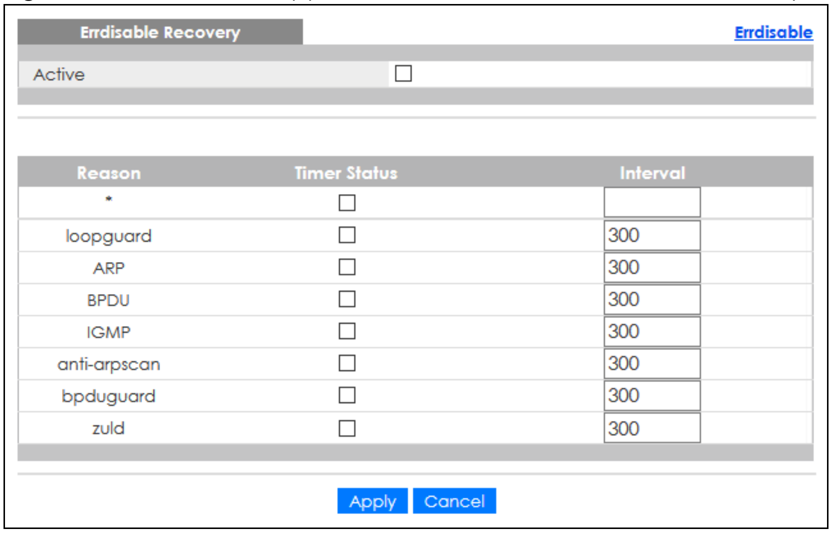
Table 155 Advanced Application > Errdisable > Errdisable Detect

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. 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 drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** – The Switch drops the additional control packets the ports 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.

33.6 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 238 Advanced Application > Errdisable > Errdisable Recovery



The following table describes the labels in this screen.

Table 156 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. Changes in this row are copied to all the entries as soon as you make them.
Timer Status	Select this check box 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. Clear the check box 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.

CHAPTER 34
VLAN Isolation

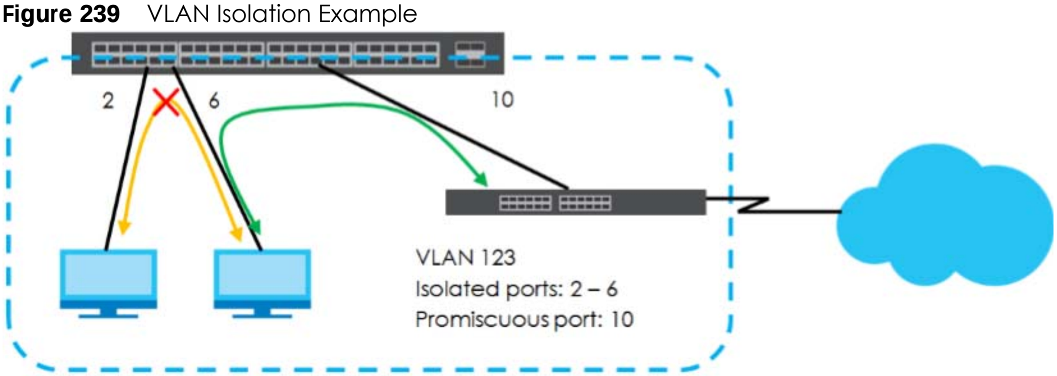
This chapter shows you how to configure the Switch to prevent communications between ports in a VLAN.

34.1 VLAN Isolation Overview

Vlan Isolation allows you to do port isolation within a VLAN in a simple way. You specify which ports in a VLAN is not isolated by adding it to the promiscuous port list. The Switch automatically adds other ports in this VLAN to the isolated port list and blocks traffic between the isolated ports. A promiscuous port can communicate with any port in the same VLAN. An isolated port can communicate with the promiscuous ports only.

Note: You can have up to one VLAN Isolation rule for each VLAN.

Figure 239 VLAN Isolation Example

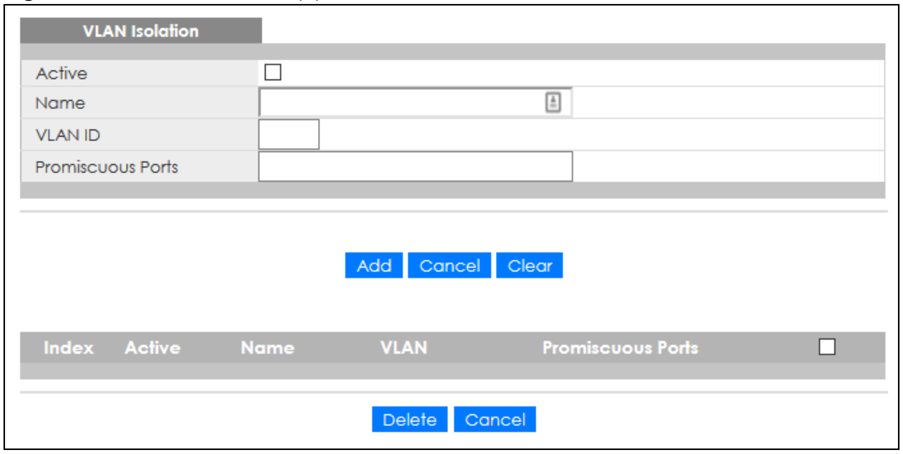


Note: Make sure you keep at least one port in the promiscuous port list for a VLAN with VLAN Isolation enabled. Otherwise, this VLAN is blocked from the whole network.

34.2 Configuring VLAN Isolation

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

Figure 240 Advanced Application > Vlan Isolation



The following table describes the labels in this screen.

Table 157 Advanced Application > Vlan Isolation

LABEL	DESCRIPTION
Active	Check this box to enable VLAN Isolation in a VLAN.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
VLAN ID	Enter a VLAN ID from 1 to 4094. This is the VLAN to which this rule applies.
Promiscuous Ports	Enter the number of the ports that can communicate with any ports in the same VLAN. Other ports belonging to this VLAN will be added to the isolation list and can only send and receive traffic from the ports you specify here.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **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 clear the fields to the factory defaults.
Index	This is the index number of the rule.
Active	This shows whether this rule is activated or not.
Name	This is the descriptive name for this rule.
VLAN	This is the VLAN to which this rule is applied.
Promiscuous Ports	This shows the ports that can communicate with any ports in the same 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 rules that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the check boxes.

CHAPTER 35 Green Ethernet

This chapter shows you how to configure the Switch to reduce the power consumed by switch ports.

35.1 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

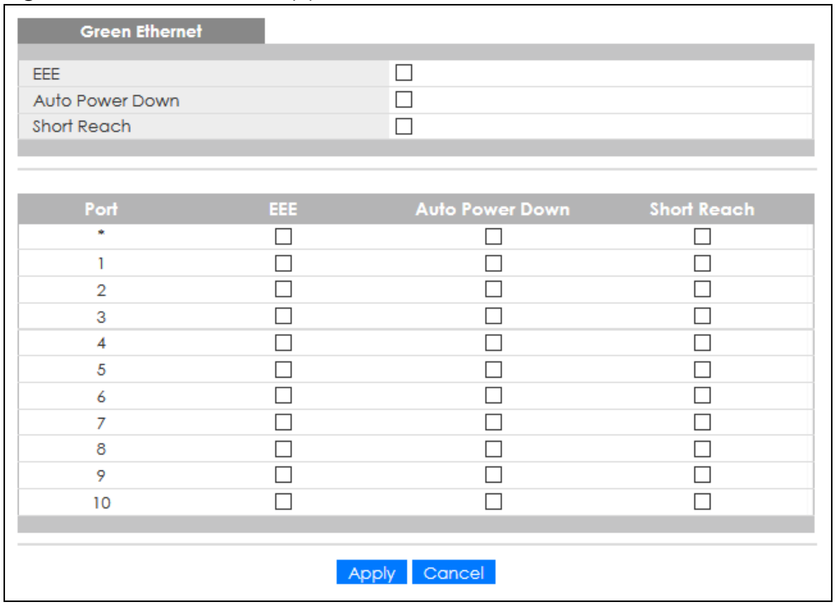
Traditional Ethernet transmits all data with enough power to reach the maximum cable length. Shorter cables lose less power, so **Short Reach** saves power by adjusting the transmit power of each port according to the length of cable attached to that port.

35.2 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 241 Advanced Application > Green Ethernet



The following table describes the labels in this screen.

Table 158 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.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. 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.

CHAPTER 36
Link Layer Discovery Protocol (LLDP)

36.1 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)

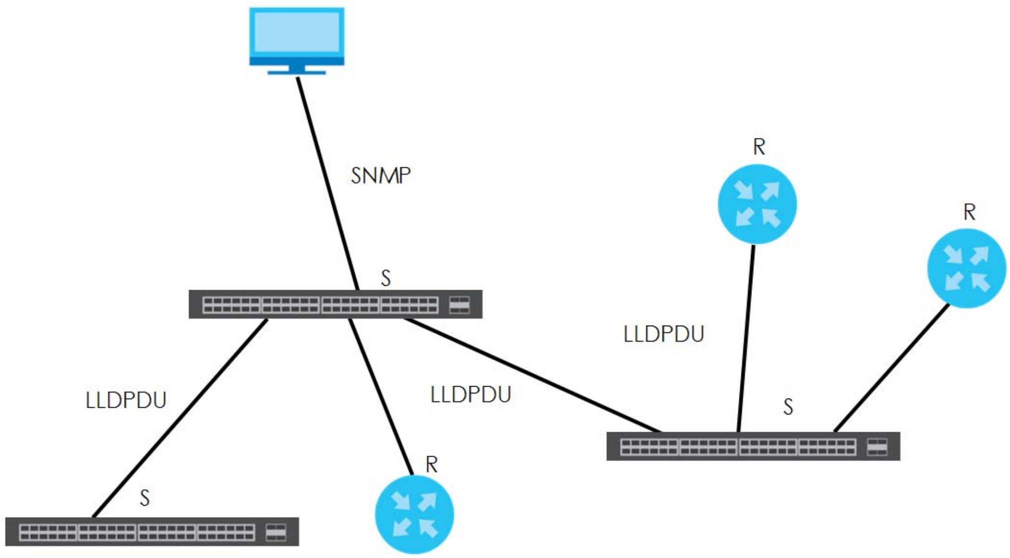
IEEE 802.3 specific TLVs:

- 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 242 LLDP Overview



36.2 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 mis-configured IP addresses. There are three classes of endpoint devices that the LLDP-MED supports:

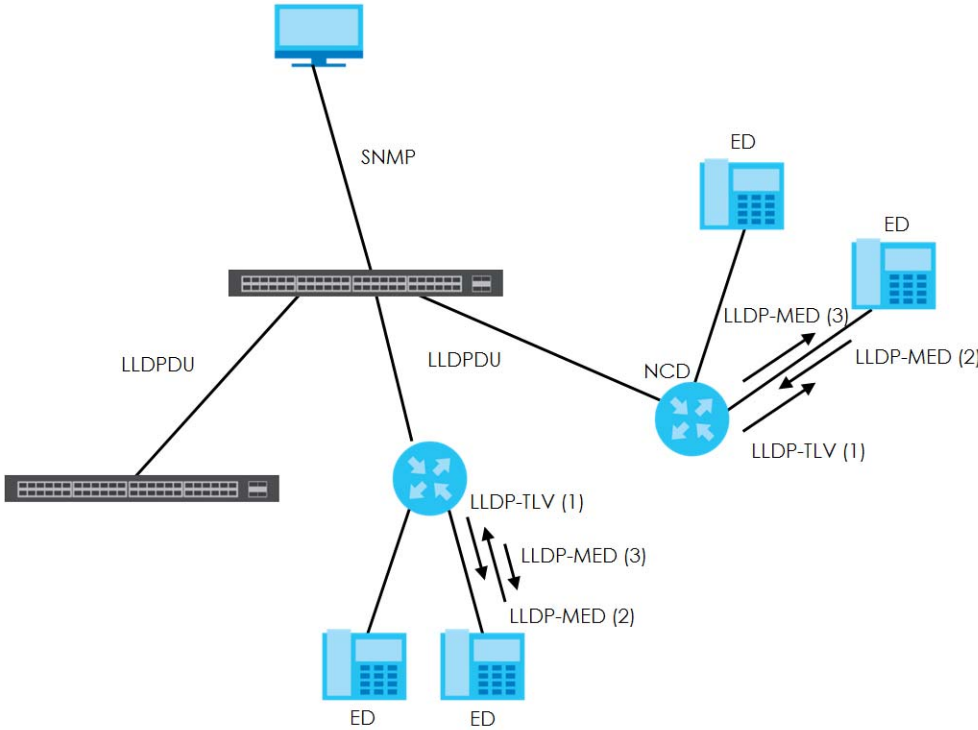
Class I: IP Communications Controllers or other communication related servers

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.

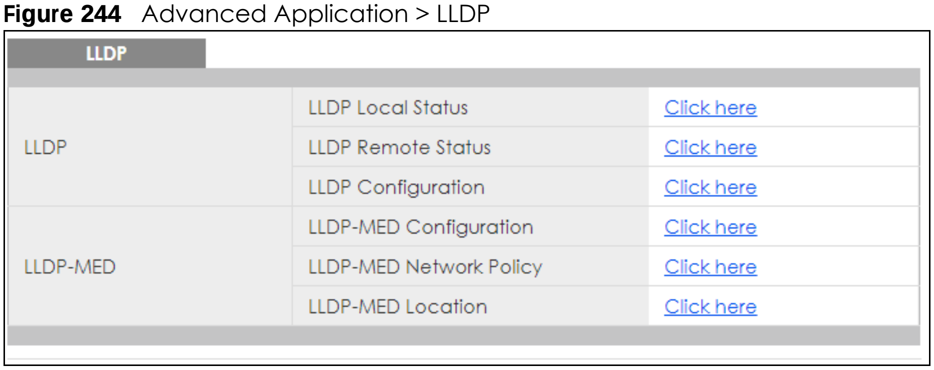
Figure 243 LLDP-MED Overview



36.3 LLDP Settings

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

Figure 244 Advanced Application > LLDP



LLDP

LLDP	LLDP Local Status	Click here
	LLDP Remote Status	Click here
	LLDP Configuration	Click here
LLDP-MED	LLDP-MED Configuration	Click here
	LLDP-MED Network Policy	Click here
	LLDP-MED Location	Click here

The following table describes the labels in this screen.

Table 159 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.

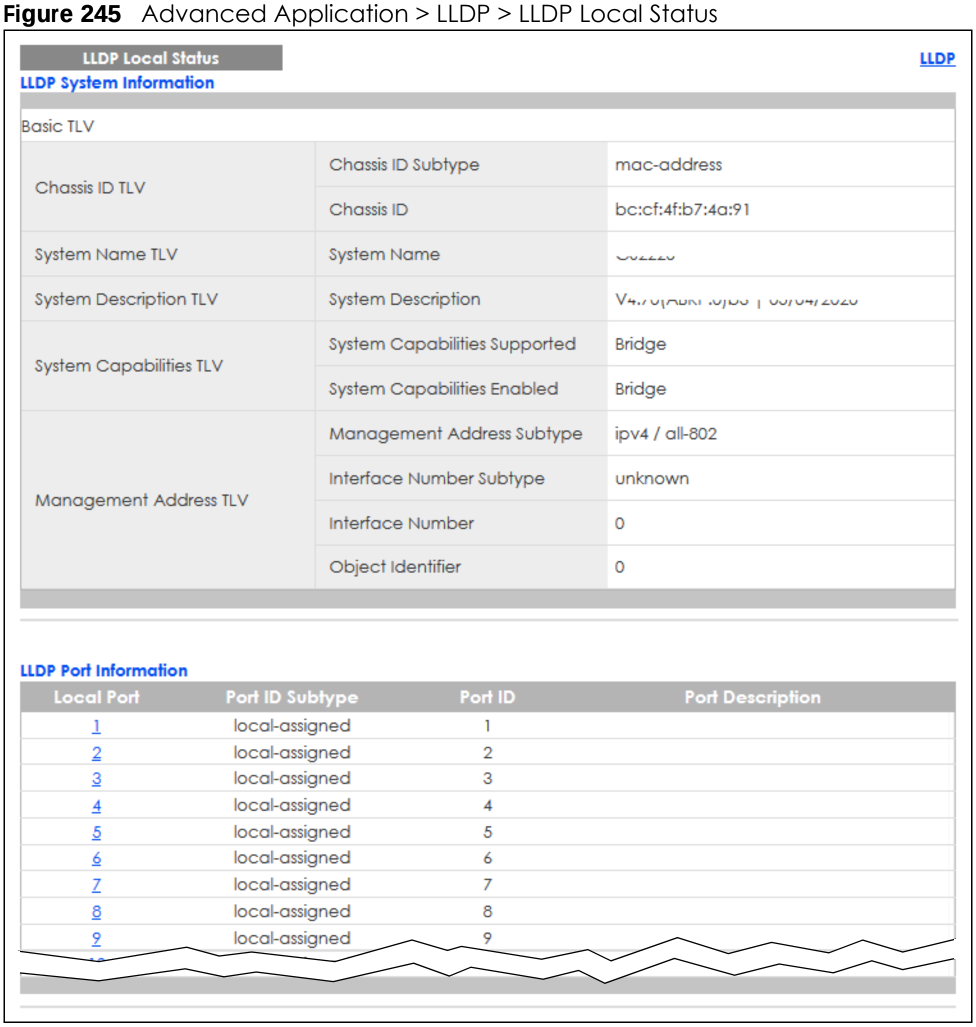
Table 159   Advanced Application > LLDP (continued)

LABEL	DESCRIPTION
LLDP Configuration	Click here to show a screen to configure LLDP parameters.
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.

36.4 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 245   Advanced Application > LLDP > LLDP Local Status



The following table describes the labels in this screen.

Table 160 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 are 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
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 ports. • **Management Address Subtype** – ipv4 or 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.
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 in the **LLDP Local Port Status Detail** screen.
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.

36.4.1 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 246 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

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	port1
Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	1
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	0
Max Frame Size TLV	Max Frame Size	1518
MED TLV		
Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	
	Voice-Signaling	
	Guest-Voice	
	Guest-Voice-Signaling	
	Softphone-Voice	
	Video-Conferencing	
	Streaming-Video	
	Video-Signaling	
Location Identification TLV	Coordinate-base LCI	
	Civic LCI	
	ELIN	

The following table describes the labels in this screen.

Table 161 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LABEL	DESCRIPTION
Local Port	This displays the number of the Switch's port.
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.
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.
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

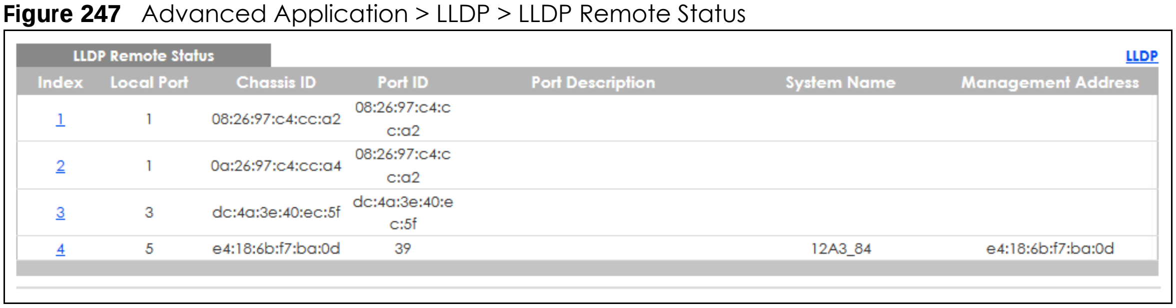
Table 161 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (continued)

LABEL	DESCRIPTION
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-based 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)

36.5 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 (Click Here)** to display the screen as shown next.

Figure 247 Advanced Application > LLDP > LLDP Remote Status



The following table describes the labels in this screen.

Table 162 Advanced Application > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
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.
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.

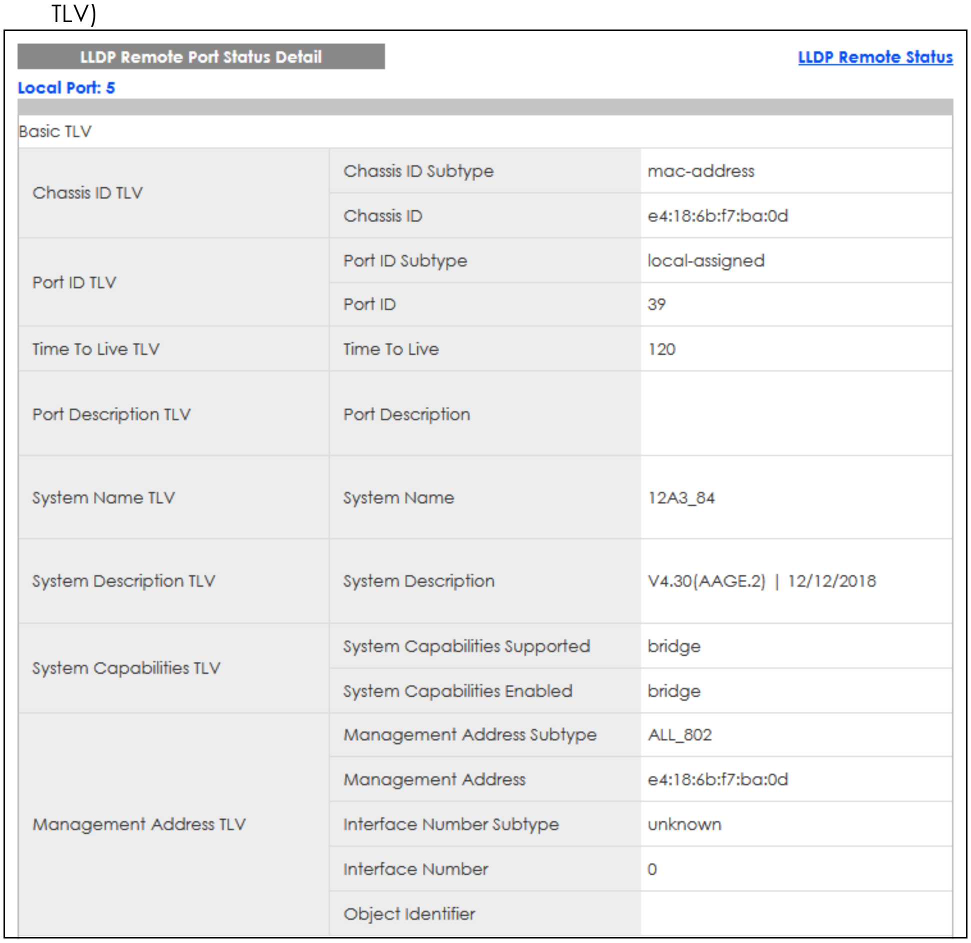
Table 162 Advanced Application > LLDP > LLDP Remote Status (continued)

LABEL	DESCRIPTION
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.

36.5.1 LLDP Remote Port Status Detail

This screen displays detailed LLDP status of the remote device connected to the Switch. Click **Advanced Application** > **LLDP** > **LLDP Remote Status (Click Here)** 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 248 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 163 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	

Table 163 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV) (continued)

LABEL	DESCRIPTION
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.
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 management address of the remote device. • **Management Address Subtype** • **Management Address** • **Interface Number Subtype** • **Interface Number** • **Object Identifier**

Figure 249 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail> (Dot 1 and Dot3 TLV)

Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	
	Port-Protocol VLAN ID Supported	
	Port-Protocol VLAN ID Enabled	
Vlan Name TLV	VLAN ID	
	VLAN Name	
Protocol Identity TLV	Protocol ID	
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	No
	AN Enabled	No
	AN Advertised Capability	
	Oper MAU type	0
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	No
	Aggregated Port ID	0
Power Via MDI TLV	Port Class	
	MDI Supported	
	MDI Enabled	
	Pair Controlable	
	PSE Power Pairs	
	Power Class	
Max Frame Size TLV	Max Frame Size	

The following table describes the labels in the Dot1 and Dot3 parts of the screen.

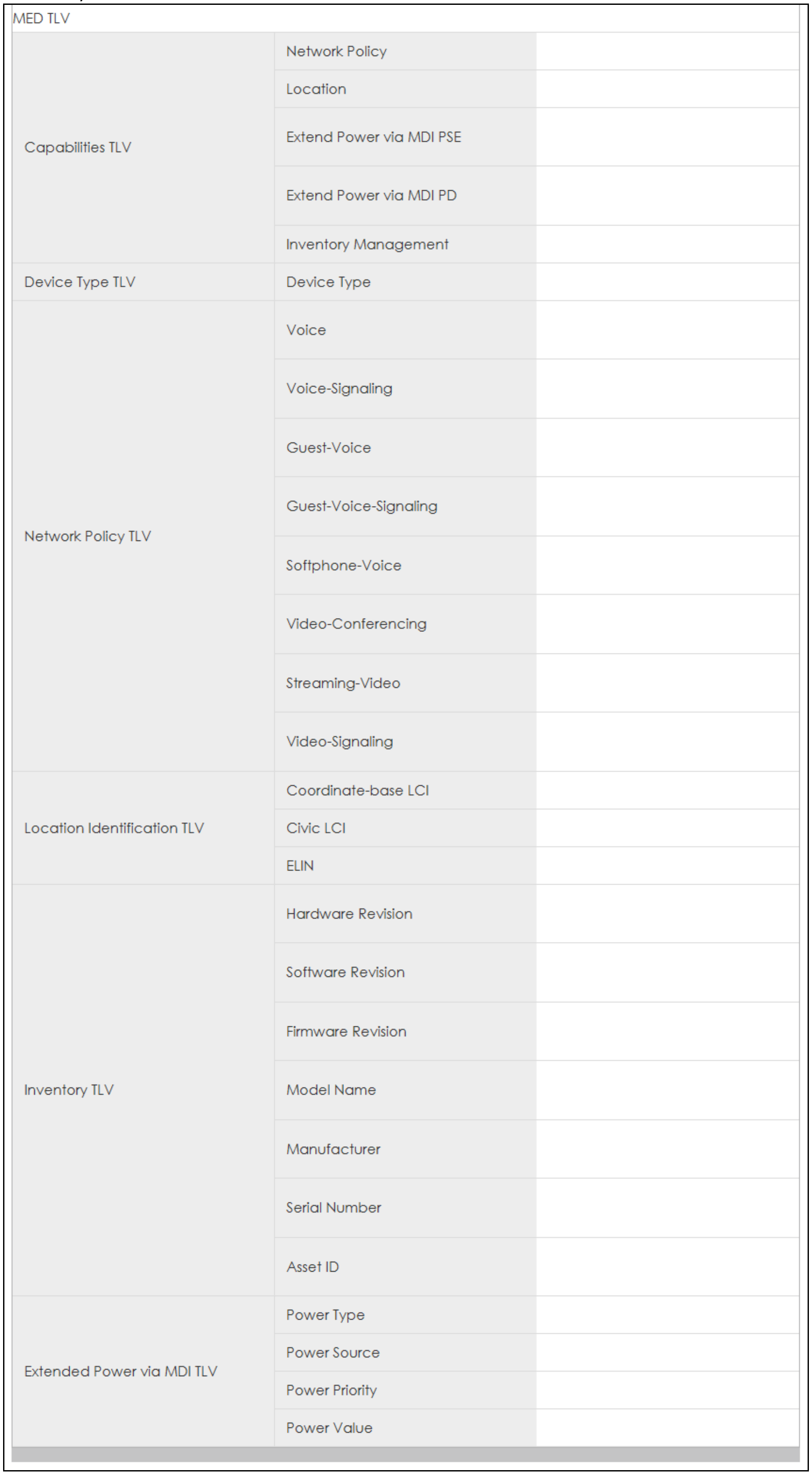
Table 164 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

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**

Table 164   Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV) (continued)

LABEL	DESCRIPTION
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 Controllable** • **PSE Power Pairs** • **Power Class**
Max Frame Size TLV	This displays the maximum supported frame size in octets.

Figure 250 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 165 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)
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.

36.6 LLDP Configuration

Use this screen to configure global LLDP settings on the Switch. Click **Advanced Application** > **LLDP** > **LLDP Configuration (Click Here)** to display the screen as shown next.

Figure 251 Advanced Application > LLDP > LLDP Configuration

The following table describes the labels in this screen.

Table 166 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.
Port	This displays the Switch's port number. * means all ports.
*	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. Changes in this row are copied to all the ports as soon as you make them.

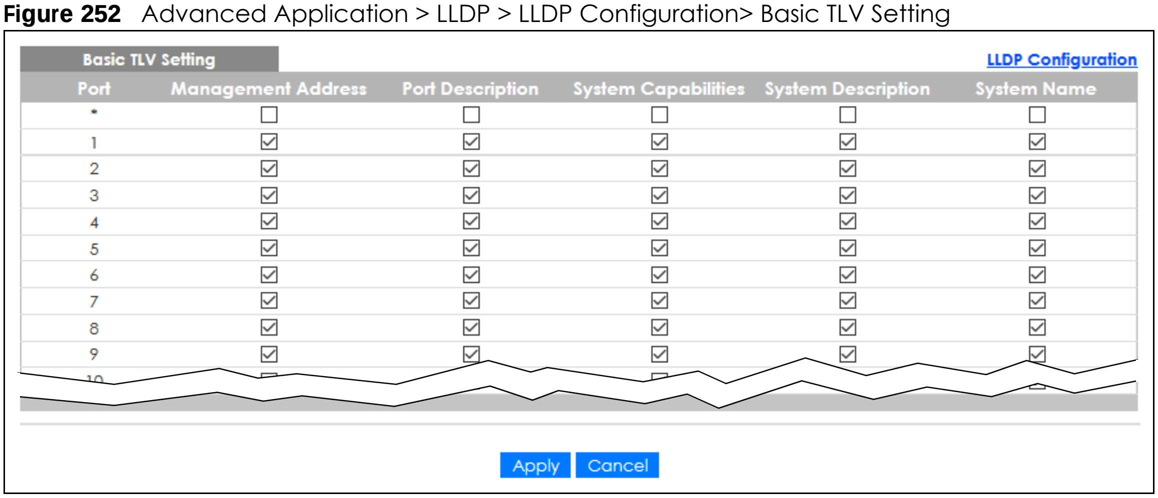
Table 166 Advanced Application > LLDP > LLDP Configuration (continued)

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.

36.6.1 LLDP Configuration Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **Advanced Application** > **LLDP** > **LLDP Configuration (Click Here)** > **Basic TLV Setting** to display the screen as shown next.

Figure 252 Advanced Application > LLDP > LLDP Configuration> Basic TLV Setting



The following table describes the labels in this screen.

Table 167 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

LABEL	DESCRIPTION
Port	This 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 to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Management Address	Select the check boxes to enable or disable the sending of Management Address TLVs on the ports.
Port Description	Select the check boxes to enable or disable the sending of Port Description TLVs on the ports.
System Capabilities	Select the check boxes to enable or to disable the sending of System Capabilities TLVs on the ports.
System Description	Select the check boxes to enable or to disable the sending of System Description TLVs on the ports.

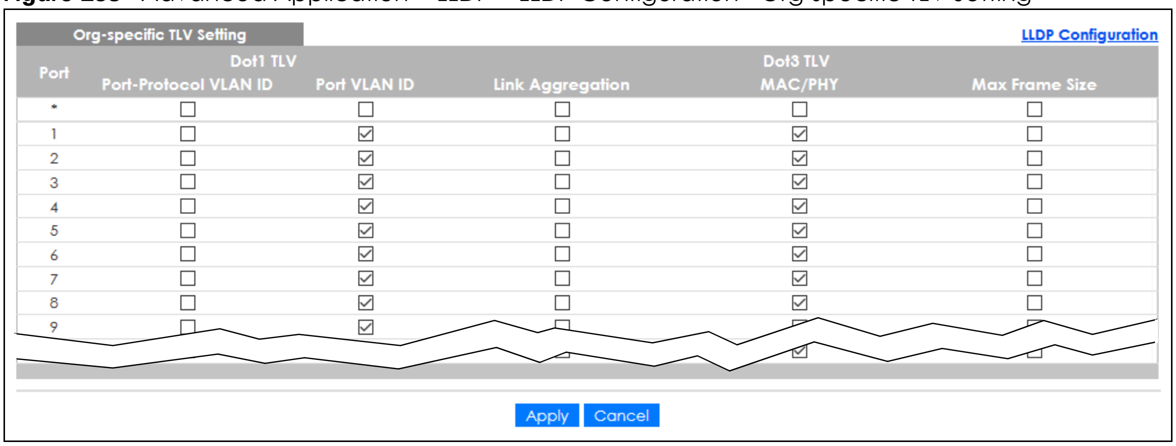
Table 167 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting (continued)

LABEL	DESCRIPTION
System Name	Select the check boxes to enable or to disable the sending of System Name TLVs on the 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.

36.6.2 LLDP Configuration Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **Advanced Application** > **LLDP** > **LLDP Configuration (Click Here)** > **Org-specific TLV Setting** to display the screen as shown next.

Figure 253 Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting



The following table describes the labels in this screen.

Table 168 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

LABEL	DESCRIPTION
Port	This 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 to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Dot1 TLV	
Port-Protocol VLAN ID	Select the check boxes to enable or disable the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs on the ports.
Port VLAN ID	Select the check boxes to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the ports. All check boxes in this column are enabled by default.
Dot3 TLV	
Link Aggregation	Select the check boxes to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the ports.
MAC/PHY	Select the check boxes to enable or disable the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the ports. All check boxes in this column are enabled by default.
Max Frame Size	Select the check boxes to enable or disable the sending of IEEE 802.3 Max Frame Size TLVs on the ports.

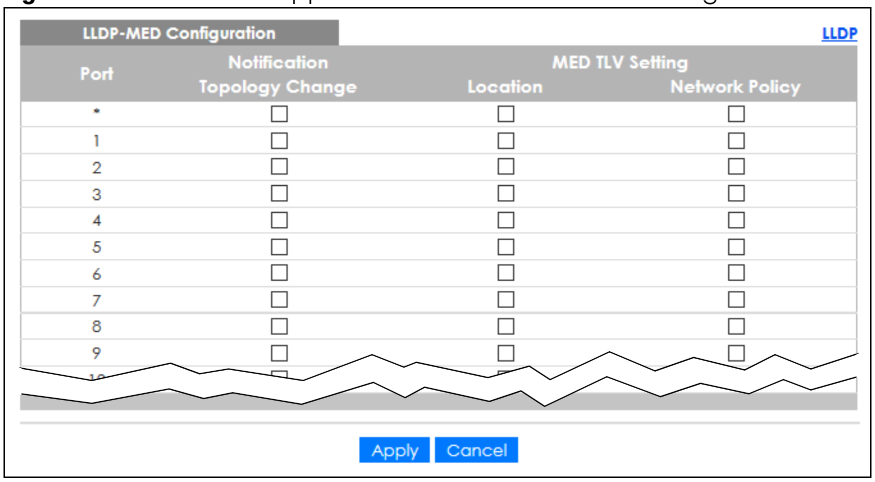
Table 168   Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

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.

36.7 LLDP-MED Configuration

Click **Advanced Application** > **LLDP** > **LLDP-MED Configuration** to display the screen as shown next.

Figure 254   Advanced Application > LLDP > LLDP-MED Configuration



The following table describes the labels in this screen.

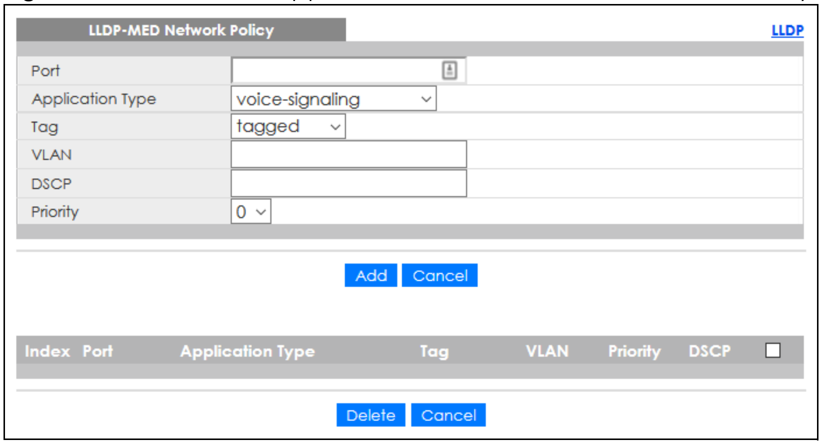
Table 169   Advanced Application > LLDP > LLDP-MED Configuration

LABEL	DESCRIPTION
Port	This displays the Switch's port number. Select * to configure all ports simultaneously.
*	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. Changes in this row are copied to all the ports as soon as you make them.
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.

36.8 LLDP-MED Network Policy

Click **Advanced Application** > **LLDP** > **LLDP-MED Network Policy (Click Here)** to display the screen as shown next.

Figure 255 Advanced Application > LLDP > LLDP-MED Network Policy



The following table describes the labels in this screen.

Table 170 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
Port	Enter the port number to set up the LLDP-MED network policy.
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 have 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.
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.

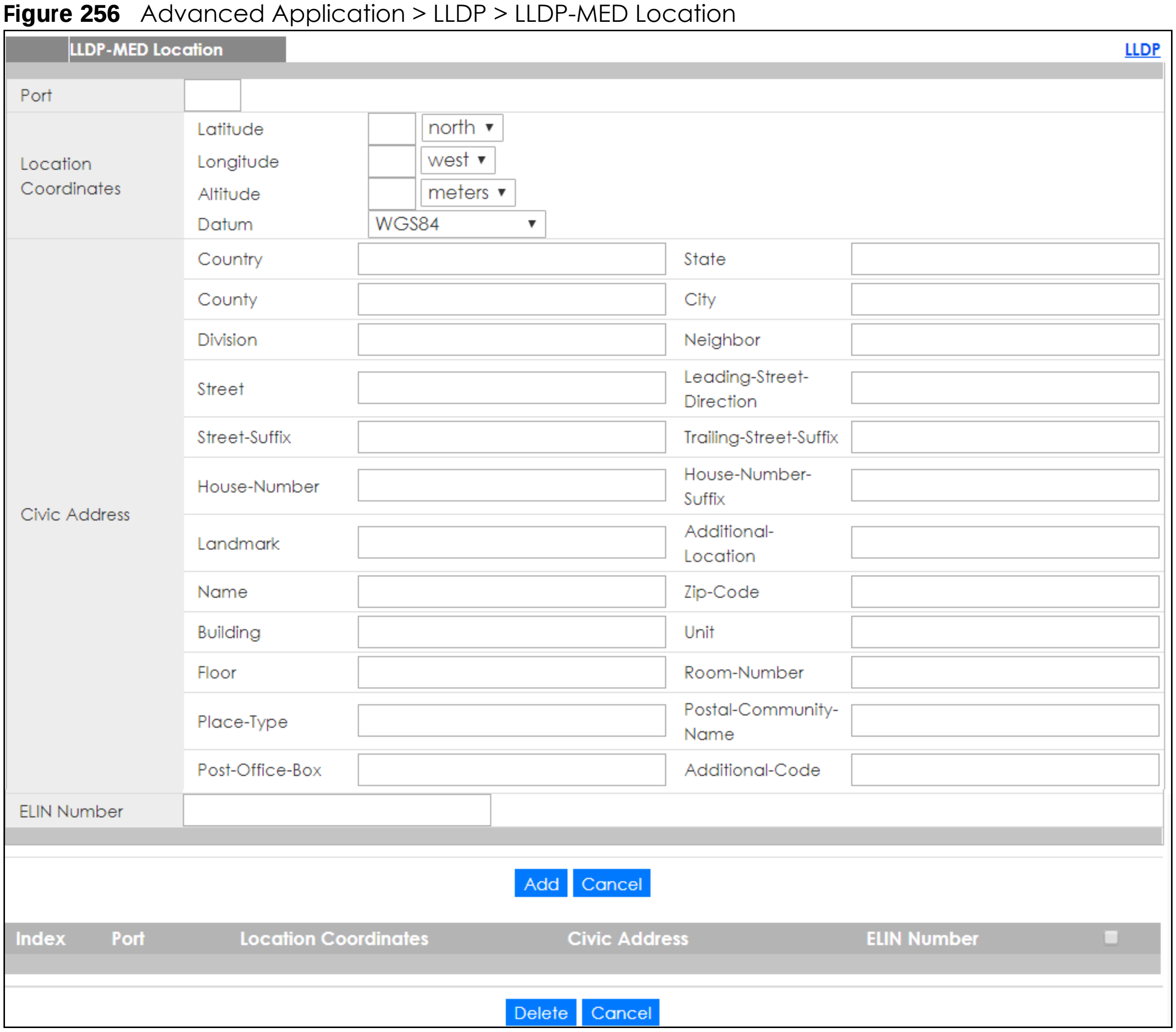
Table 170   Advanced Application > LLDP > LLDP-MED Network Policy (continued)

LABEL	DESCRIPTION
Priority	This field displays the priority value of the network policy.
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 check boxes.

36.9 LLDP-MED Location

Click **Advanced Application** > **LLDP** > **LLDP-MED Location (Click Here)** to display the screen as shown next.

Figure 256   Advanced Application > LLDP > LLDP-MED Location



The following table describes the labels in this screen.

Table 171 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.
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 0° to 90°. The negative value represents the South. • **north** • **south**
Longitude	Enter the longitude information. The value should be from 0° to 180°. The negative value represents the West. • **west** • **east**
Altitude	Enter the altitude information. The value should be from –2097151 to 2097151 in meters or in floors. • **meters** • **floor**
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 2 fields 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**

Table 171   Advanced Application > LLDP > LLDP-MED Location (continued)

LABEL	DESCRIPTION
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 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.
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 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.
Delete	Check the locations that you want to remove, then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

CHAPTER 37
Anti-Arpscan

37.1 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.

37.1.1 What You Can Do

- Use the **Anti-Arpscan Status** screen (Section 37.2 on page 345) to see what ports are trusted and are forwarding traffic or are disabled.
- Use the **Anti-Arpscan Host Status** screen (Section 37.3 on page 345) to view blocked hosts and clear selected ones.
- Use the **Anti-Arpscan Trust Host** screen (Section 37.4 on page 346) 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 37.5 on page 347) to enable anti-arpscan, set port and host thresholds as well as configure ports to be trusted or untrusted.

37.1.2 What You Need to Know

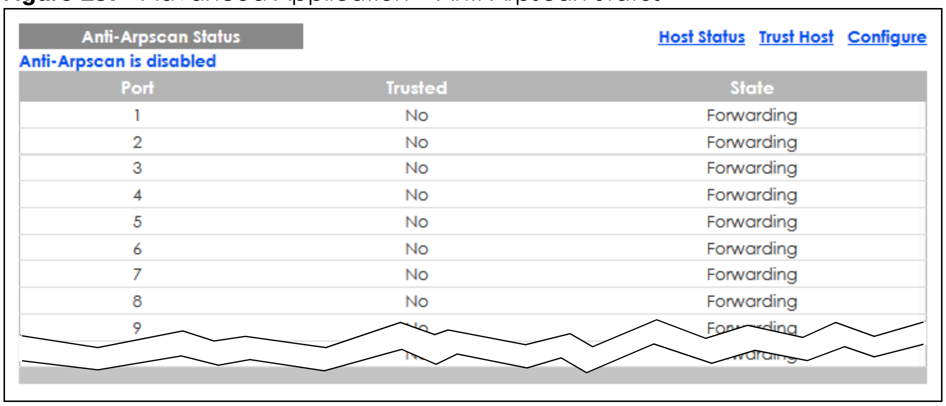
- You should set an uplink port as a trusted port before enabling **Anti-arpscan** so as to prevent the port from being shutdown due to receiving too many ARP messages.
- When a port is configured as a trusted port, **Anti-arpscan** is not performed on the port. Both host and port thresholds are ignored 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 ports 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.

37.2 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 257 Advanced Application > Anti-Arpscan Status



The following table describes the fields in the above screen.

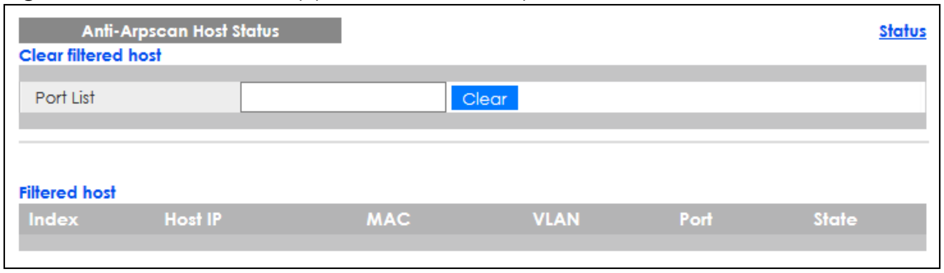
Table 172 Advanced Application > Anti-Arpscan Status

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**).

37.3 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 258 Advanced Application > Anti-Arpscan > Host Status



The following table describes the fields in the above screen.

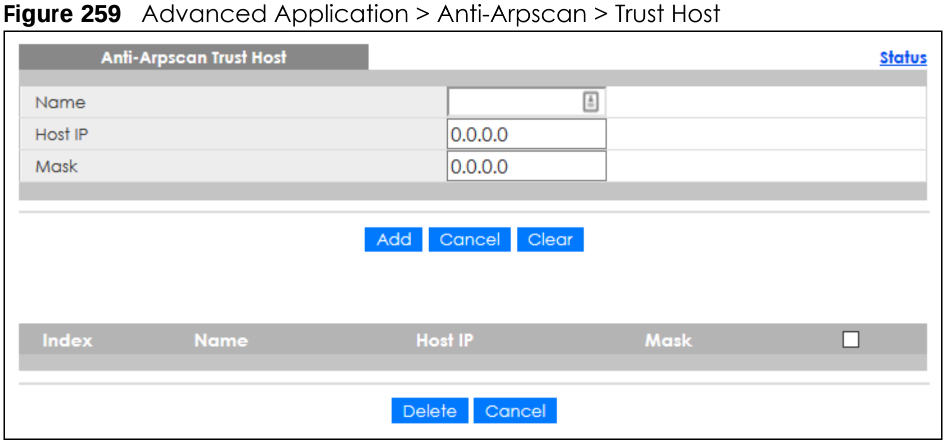
Table 173 Advanced Application > Anti-Arpscan > Host Status

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.

37.4 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 259 Advanced Application > Anti-Arpscan > Trust Host



The following table describes the fields in the above screen.

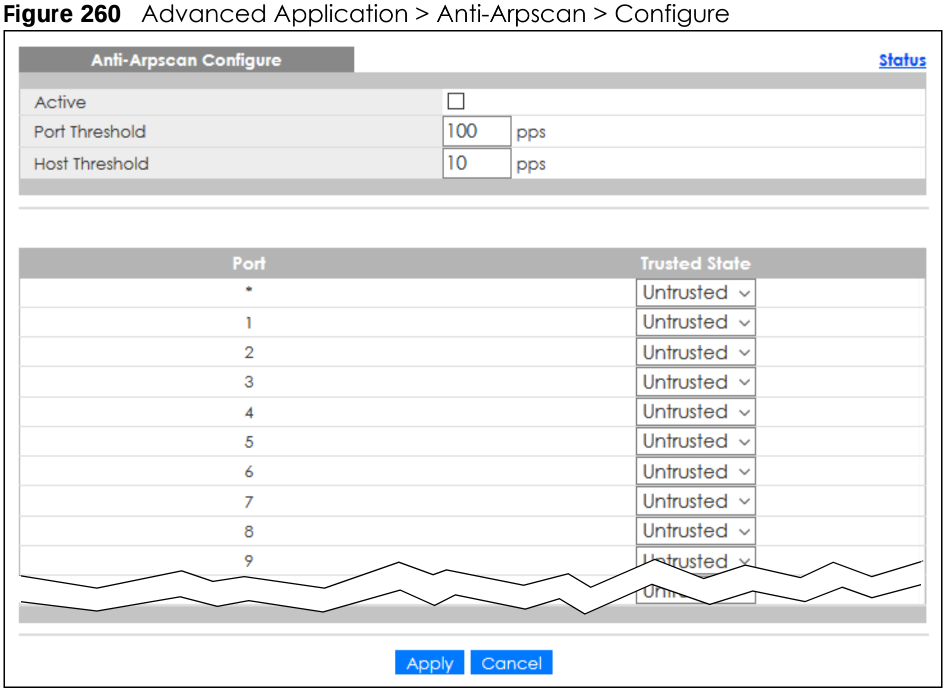
Table 174   Advanced Application > Anti-Arpscan > Trust Host

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 check box and click **Delete** to remove the specified entry.
Cancel	Click this to clear the check boxes above.

37.5 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 260   Advanced Application > Anti-Arpscan > Configure



The following table describes the fields in the above screen.

Table 175 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	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Trusted State	Select **Untrusted** or **Trusted** for the associated port. **Anti-arpscan** is not performed on trusted hosts.
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.

CHAPTER 38
BPDU Guard

38.1 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 ports on which BPDU guard is enabled, the Switch disables the ports automatically. You can then enable the ports manually in the **Basic Setting** > **Port Setup** screen, or use the **Errdisable Recovery** screen (see Section 33.6 on page 316) to have the ports become active after a certain time interval.

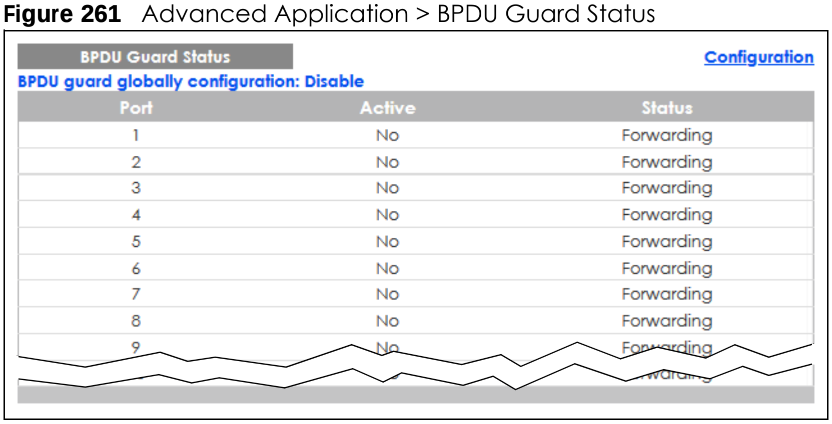
38.1.1 What You Can Do

- Use the **BPDU Guard Status** screen (Section 38.2 on page 349) to view the BPDU guard status.
- Use the **BPDU Guard Configuration** screen (Section 38.3 on page 350) to enable BPDU guard on the Switch.

38.2 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 261 Advanced Application > BPDU Guard Status



The following table describes the fields in the above screen.

Table 176   Advanced Application > BPDU Guard Status

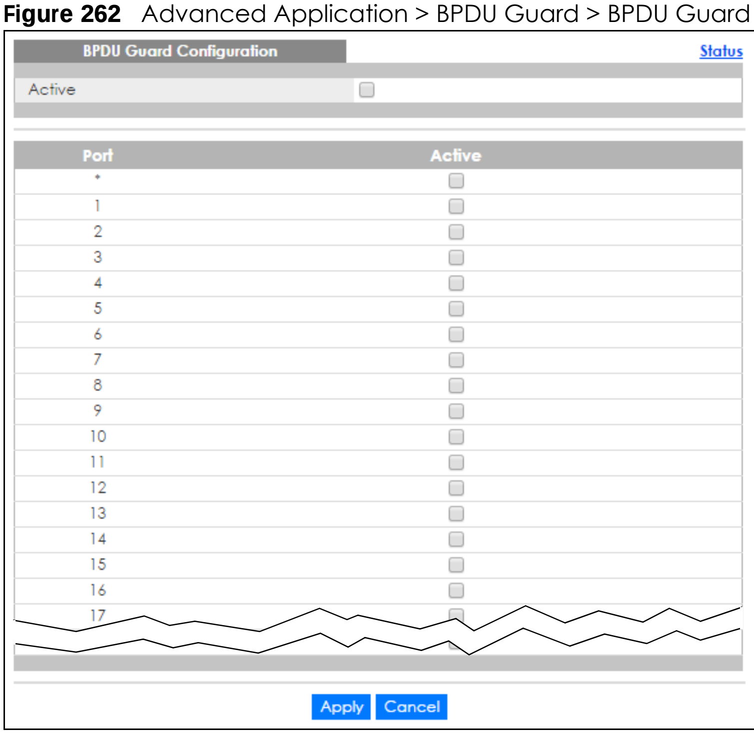
LABEL	DESCRIPTION
BPDU guard globally configuration	This field displays whether BPDU guard is activated on the Switch.
Port	This field displays the port number.
Active	This shows whether BPDU guard is activated on the port.
Status	This shows whether the port is shut down (**Err-disable**) or able to transmit packets (**Forwarding**).

38.3 BPDU Guard Configuration

Use this screen to turn on the BPDU guard feature on the Switch and ports.

In the **BPDU Guard Status** screen, click **Configuration** to display the configuration screen as shown.

Figure 262   Advanced Application > BPDU Guard > BPDU Guard Configuration



The following table describes the fields in the above screen.

Table 177   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 port number.

Table 177   Advanced Application > BPDU Guard > BPDU Guard Configuration (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.
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.

CHAPTER 39
OAM

39.1 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.

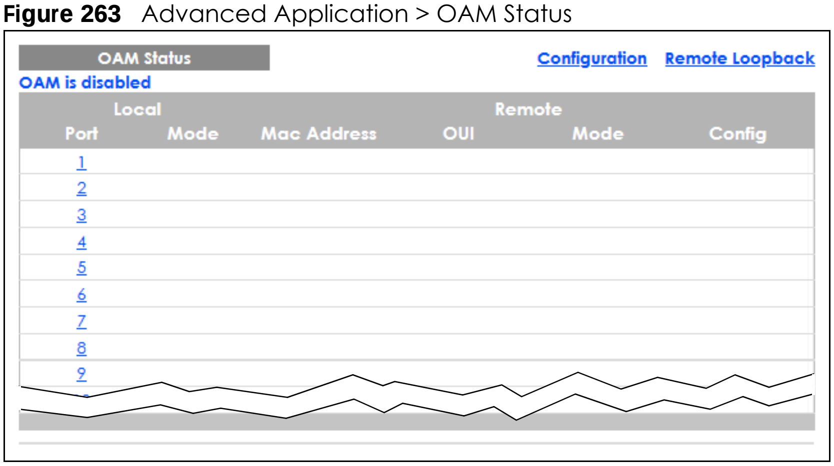
39.1.1 What You Can Do

- Use the **OAM Status** screen (Section 39.2 on page 352) to view the configuration of ports on which Ethernet OAM is enabled.
- Use the **OAM Configuration** screen (Section 39.3 on page 356) to enable Ethernet OAM on the Switch.
- Use the **OAM Remote Loopback** screen (Section 39.4 on page 357) to perform remote-loopback tests.

39.2 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 263 Advanced Application > OAM Status



The following table describes the fields in the above screen.

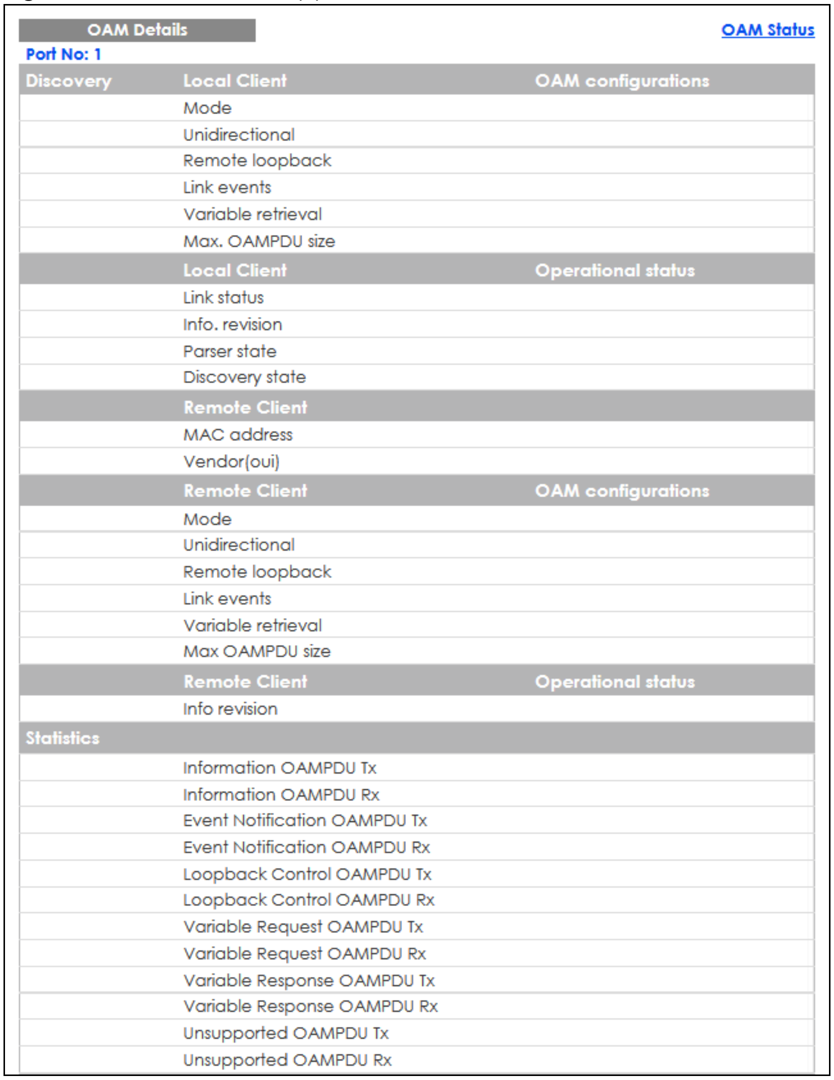
Table 178   Advanced Application > OAM Status

LABEL	DESCRIPTION
Local This section displays information about the ports on the Switch.	
Port	This field displays the port number.
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.

39.2.1 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 264 Advanced Application > OAM Status > OAM Details



The following table describes the fields in the above screen.

Table 179 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	
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.

Table 179 Advanced Application > OAM Status > OAM Details (continued)

LABEL	DESCRIPTION
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 Operational status	
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-OAM PDUs because it is trying to or has put the remote device into loopback mode.
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.
Remote Client	
MAC Address	This field displays the MAC address of the IEEE 802.3ah-enabled remote Ethernet device that is connected to the Switch.
Vendor(oui)	This field displays the Organizationally Unique Identifiers (OUI) representing the vendor of the IEEE 802.3ah-enabled remote Ethernet device that is connected to the Switch.
Statistics This section displays the number of OAM packets transferred on the port of the Switch.	

Table 179 Advanced Application > OAM Status > OAM Details (continued)

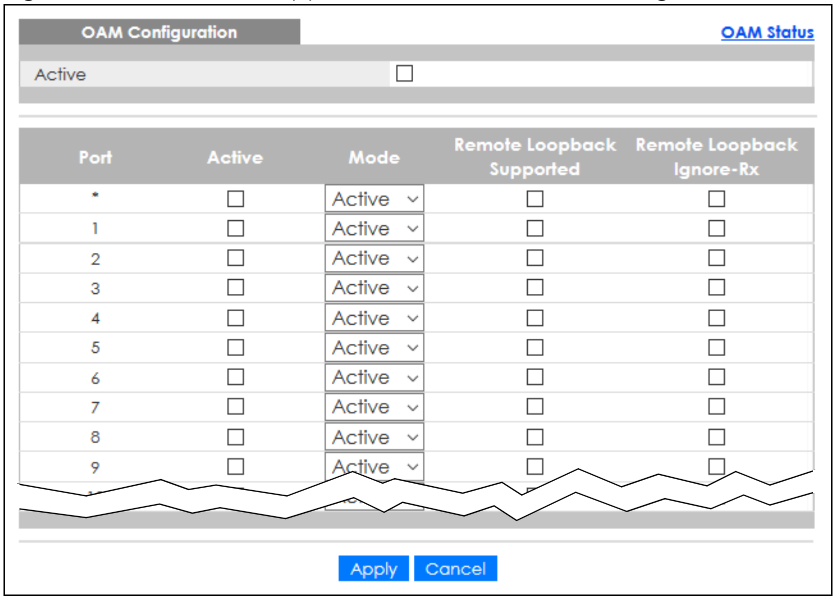
LABEL	DESCRIPTION
Information OAMPDU Tx	This field displays the number of OAM PDUs sent on the port.
Information OAMPDU Rx	This field displays the number of OAM PDUs received on the port.
Event Notification OAMPDU Tx	This field displays the number of unique or duplicate OAM event notification PDUs sent 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.

39.3 OAM Configuration

Use this screen to turn on Ethernet OAM on the Switch and ports and configure the related settings.

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

Figure 265 Advanced Application > OAM > OAM Configuration



The following table describes the fields in the above screen.

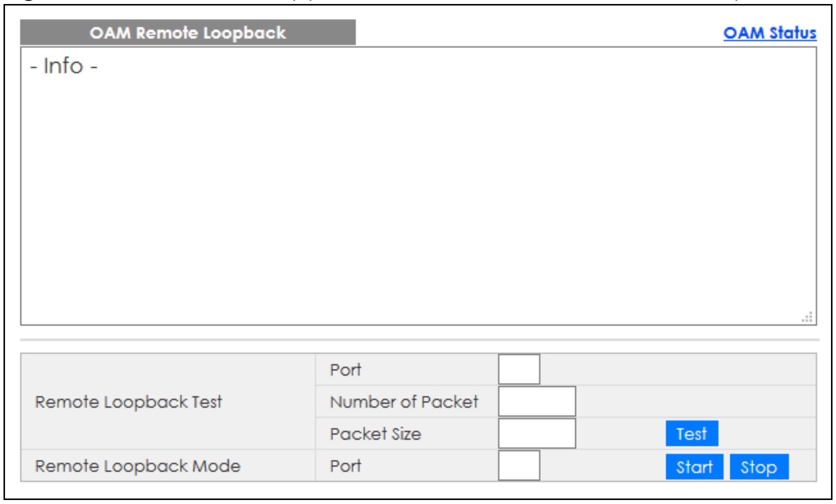
Table 180 Advanced Application > OAM > OAM Configuration

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

39.4 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 266 Advanced Application > OAM > OAM Remote Loopback



The following table describes the fields in the above screen.

Table 181 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-loopback 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.

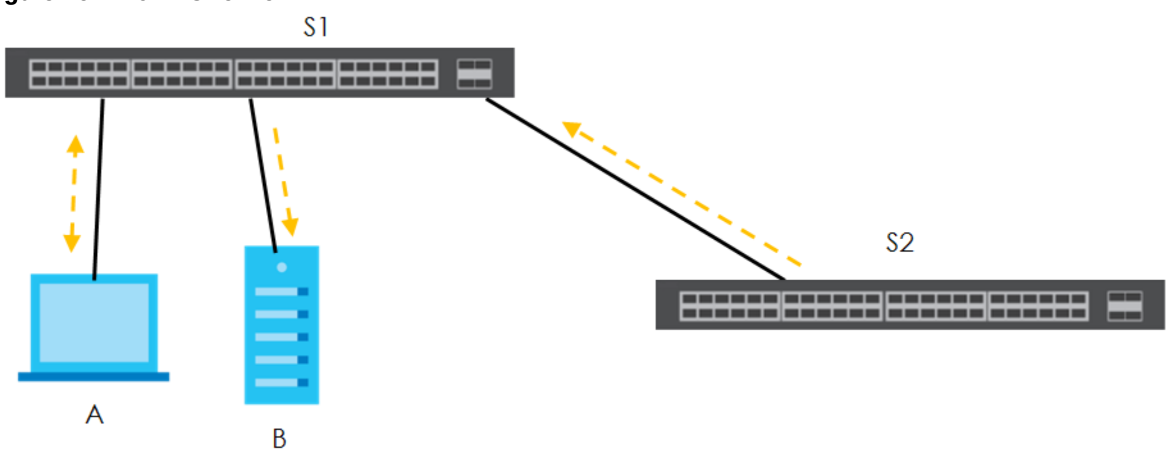
CHAPTER 40 ZULD

40.1 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 mis-configured 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 267 ZULD Overview



40.1.1 What You Can Do

- Use the **ZULD Status** screen (Section 40.2 on page 360) to see details on ZULD.
- Use the **ZULD Configuration** screen (Section 40.3 on page 361) to enable ZULD on a port, configure a mode and set the probe time.

40.1.2 What You Need to Know

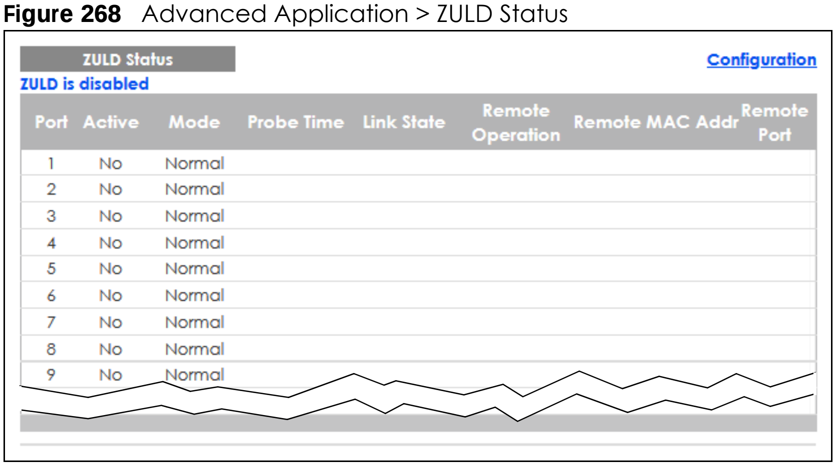
- ZULD must be enabled on the Switch and the ports in order to detect unidirectional links by monitoring OAMPDUs.
- Ports advertise their unidirectional link detection capability using OAMPDUs, so all connected devices must support **OAM** as well as **ZULD**. You need to enable OAM on the Switch by 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 (**Aggressive 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 **Advanced Application** > **Errdisable** > **Errdisable Recovery** and set the interval for **ZULD**. After the interval expires, the closed ports 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.

40.2 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 268 Advanced Application > ZULD Status



The following table describes the fields in the above screen.

Table 182 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.
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.

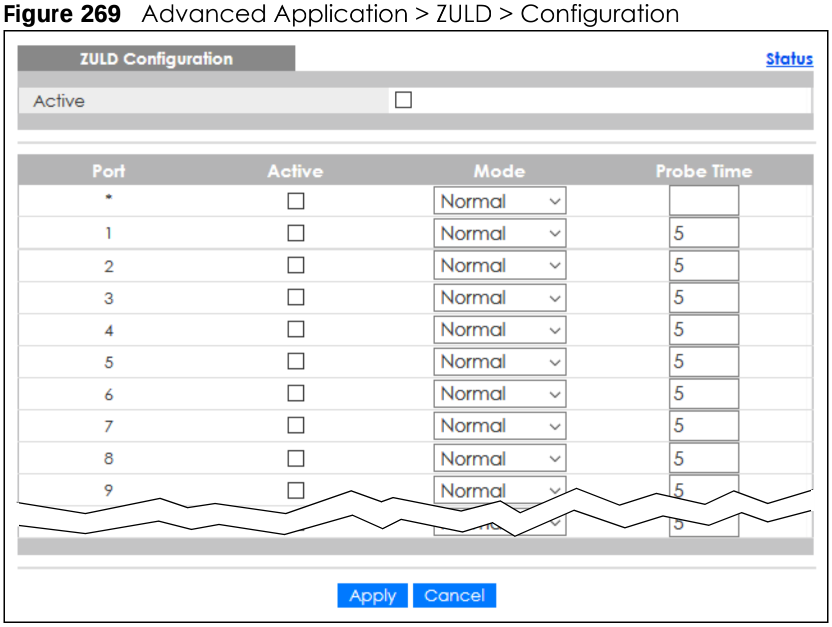
Table 182   Advanced Application > ZULD Status (continued)

LABEL	DESCRIPTION
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.
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 is 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.

40.3 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 269   Advanced Application > ZULD > Configuration



The following table describes the fields in the above screen.

Table 183   Advanced Application > ZULD > Configuration

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

CHAPTER 41
Auto PD Recovery

41.1 Auto PD Recovery Overview

Things can go wrong with any network devices. A PD (for example, IP camera) may slow down or freeze and need to be restarted if it is overworked or a bug causes a memory leak. When a connected PD ceases to respond, Automatic PD Recovery allows the Switch to restart the PD by turning it off and on without the need for on-site troubleshooting.

41.1.1 What You Can Do

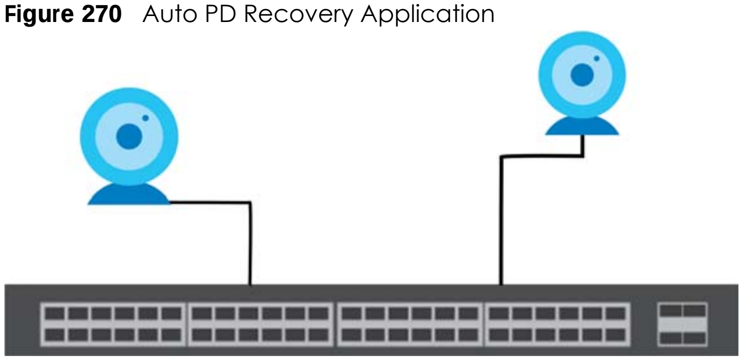
Use the **Auto PD Recovery** screen (Section 41.2 on page 363) to enable and configure automatic PD recovery on the Switch.

41.2 Auto PD Recovery

This screen lets you turn on automatic PD recovery on the Switch and its Ethernet ports. You can configure whether the Switch uses LLDP or ping to check the current status of a connected PD.

The ping is sent through the Switch's default management IP address to the designated port. To ping the PD, the port must share the same VLAN as the Switch's management VLAN.

Figure 270 Auto PD Recovery Application



The PD may stop responding to the Switch's detection over ping or LLDP during firmware upgrade. Disable the Auto PD Recovery function to prevent damage to the PD caused by a power cutoff during firmware upgrade.

To open this screen, click **Advanced Application** > **Auto PD Recovery**.

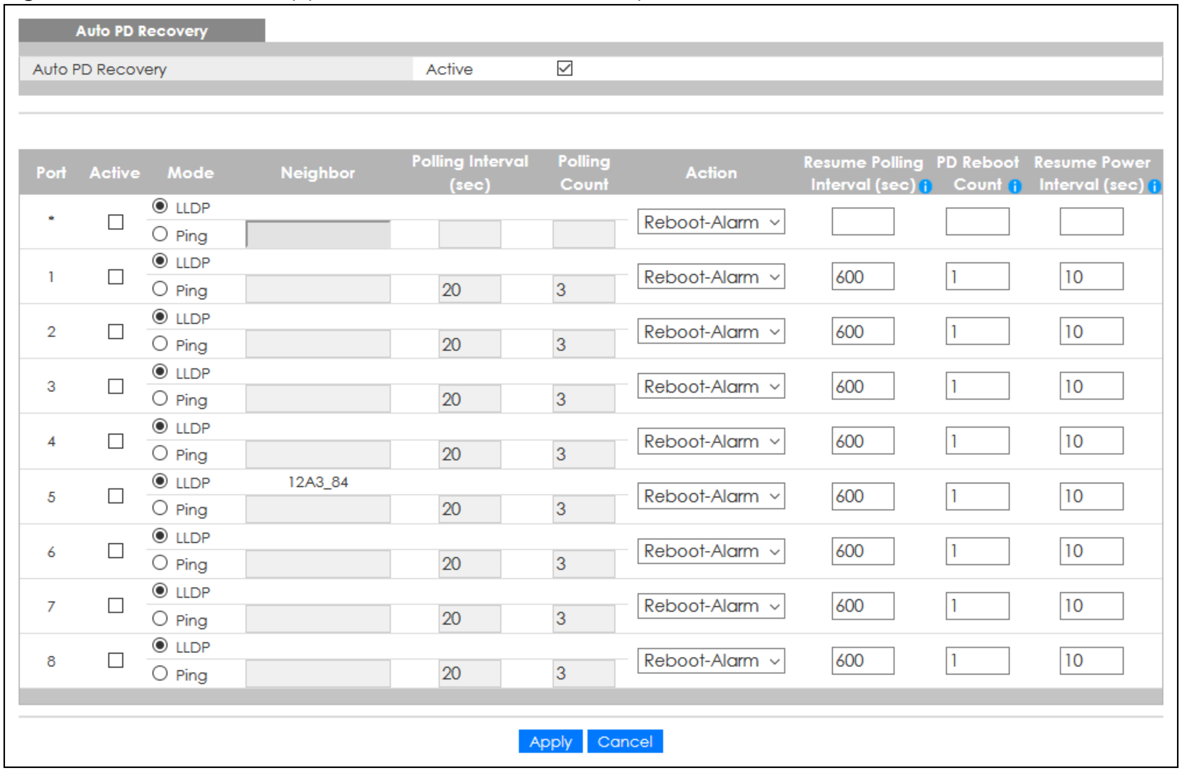


Figure 271 Advanced Application > Auto PD Recovery

The following table describes the labels in this screen.

Table 184 Advanced Application > Auto PD Recovery

LABEL	DESCRIPTION
Active	Select this option to enable Auto PD Recovery on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select **Active** to enable Auto PD Recovery on the ports.
Mode	Select **LLDP** to have the Switch passively monitor current status of the connected PD by reading LLDP packets from the PD on the port. The Switch also sends out LLDP packets to the PD to update the **Switch Neighbor** table on the PD. Select **Ping** to have the Switch ping the IP address of the connected PD to test whether the PD is reachable or not.
Neighbor	If **Mode** is set to **LLDP**, the system name of the connected PD displays automatically. If **Mode** is set to **Ping** and the PD supports LLDP, the connected PD's IPv4 or IPv6 address to which the Switch sends ping requests will display automatically. If not, enter the IP address manually.
Polling Interval	Specify the number of seconds the Switch waits for a response before sending another ping request. For example, the Switch will try to detect the PD status by performing ping requests every 20 seconds.

Table 184 Advanced Application > Auto PD Recovery (continued)

LABEL	DESCRIPTION
Polling Count	Specify how many times the Switch is to resend a ping request before considering the PD unreachable. For example, If there is no ping reply from the PD after the **Polling Interval** has elapsed, **Polling Count** starts from 1. After **Polling Count** reaches 3, the **PD Health** status LED will turn to red in the **Status** > **Neighbor** screen. The Switch will then perform your choice in the **Action** field.
Action	Set the action to take when the connected PD has stopped responding. Select **Reboot-Alarm** to have the Switch turn OFF the power of the connected PD (the connecting port is detected as link-down) and turn it back ON again to restart the PD after sending an SNMP trap and generating a log message. When restarting, the PD entry disappears from the Switch's LLDP table and the **PD Health** status LED will turn to yellow in the **Status** > **Neighbor** screen. Select **Alarm** to have the Switch send an SNMP trap and generate a log message.
Resume Polling Interval	Specify the number of seconds the Switch waits before monitoring the PD status again after it restarts the PD on the port.
PD Reboot Count	Specify how many times the Switch attempts to restart the PD on the port. The **PD Reboot Count** will reset • as soon as a ping is successful, • or when any modification to the **Auto PD Recovery** screen is applied, • or after restarting the Switch.
Resume Power Interval	Specify the number of seconds the Switch waits before supplying power to the connected PD again after it restarts the PD 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 this to reset the values in this screen to their last-saved values.

41.2.1 Activate the Automatic PD Recovery

Follow the steps below to activate the automatic PD recovery.

1 In the **Advanced Application** > **Auto PD Recovery** screen, activate the feature.

Figure 272 Auto PD Recovery (Ping Mode)

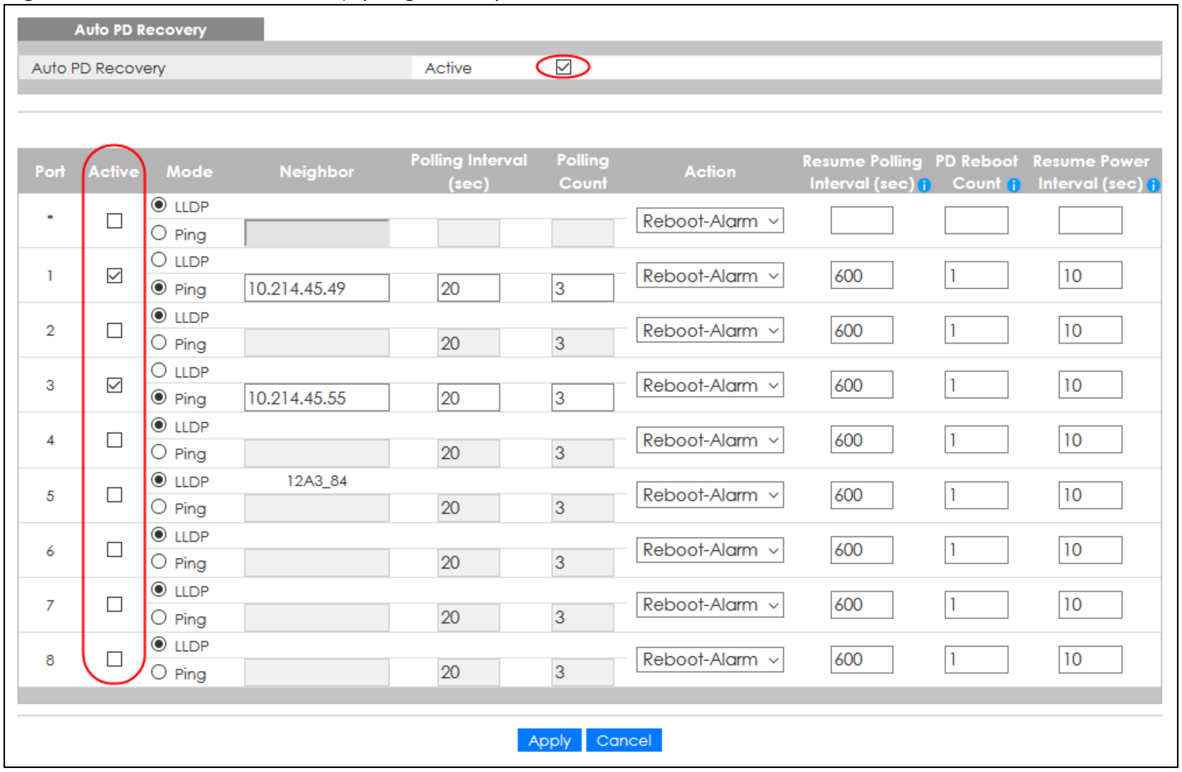
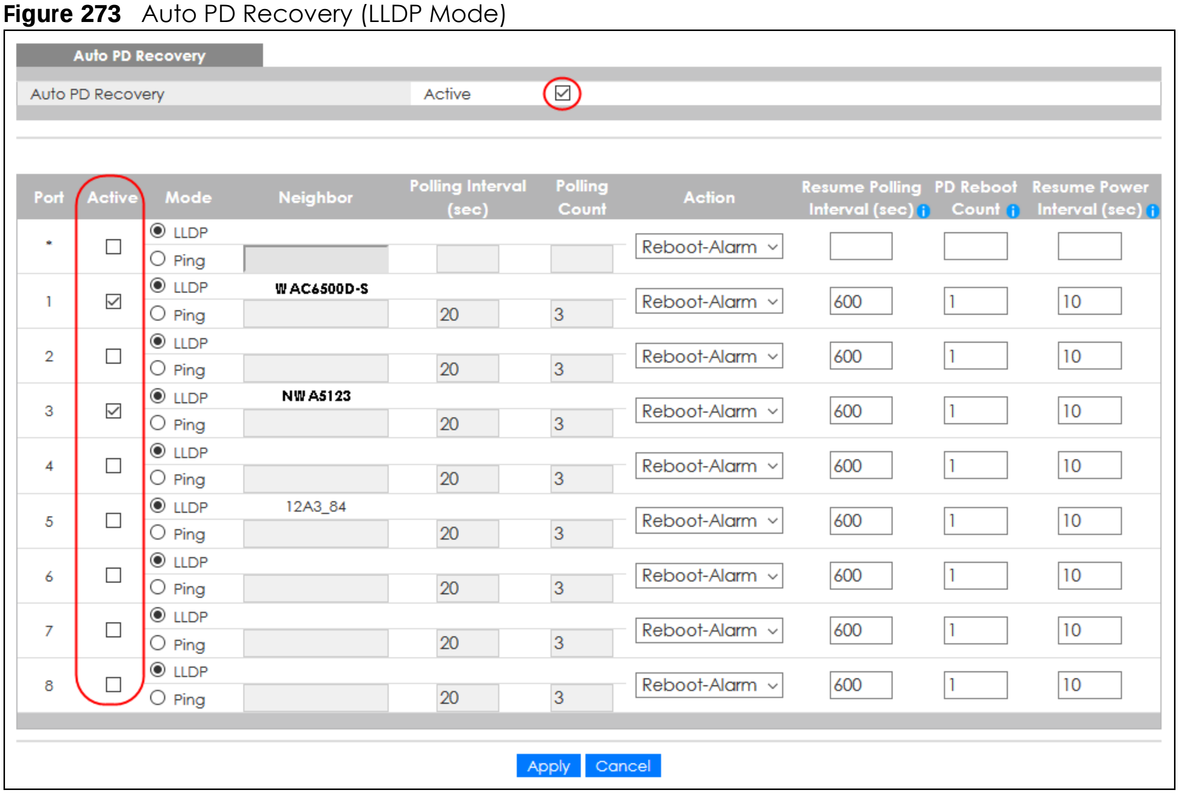


Figure 273 Auto PD Recovery (LLDP Mode)



2 Select the desired ports in the **Active** column.

3 Select the **Mode**.

When you select **Ping**, the connected PD's IPv4 or IPv6 address to which the Switch sends ping requests will display automatically if the PD supports LLDP. If not, enter the IP address of the PDs in the **Neighbor** field.

The default setting for **Polling Interval** (20 secs) and **Polling Count** (3 times) will cause the Switch to ping the PD status every 20 seconds. If there is no ping reply from the PD, **Polling Count** starts to count from 1. Once **Polling Count** reaches 3, the Switch will cause a **Reboot-Alarm** on the PD as selected in **Action**.

When you select **LLDP**, the Switch monitors the PD status by checking incoming LLDP packets every 30 seconds from the PD (default value of transmit interval for LLDP feature).

Likewise, the Switch sends out LLDP packets to the PD every 30 seconds to update the **Status** > **Neighbor** screen (see Section 7.2.1 on page 96 for details).

Once the LLDP table's counter reaches the default 120 seconds, the Switch will cause a **Reboot-Alarm** on the PD as selected in **Action**.

4 After sending an SNMP trap and generating a log message, the connected PD will restart (the connecting port is detected as link-down).

When restarting, the PD entry disappears from the Switch's LLDP table and the **PD Health** status LED will turn to yellow in the **Status** > **Neighbor** screen.

The Switch will restore power to the PD based on your value for **Resume Power Interval**.

After the PD is powered on, the Switch resumes detection of the PD status by performing ping requests or checking the LLDP table based on your value for **Resume Polling Interval**.

When the **PD Reboot Count** value is reached, the Switch will no longer perform the PD recovery process. The **PD Health** status LED will turn to red in the **Status** > **Neighbor** screen.

5 Click **Apply** to save your changes back to the run-time memory.

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

Note: In the event of a PD performing firmware upgrade, the PD may stop responding to ping or fail to provide LLDP packets for an extended period of time. When the Switch resets power to the PD before firmware upgrade is finished, it may permanently damage the PD or require a hard reset to recover it. **It is strongly advised to disable the Switch's Auto PD Recovery function before upgrading the PD's firmware. This will prevent damage caused by a power cutoff.**

CHAPTER 42
Static Route

42.1 Static Routing

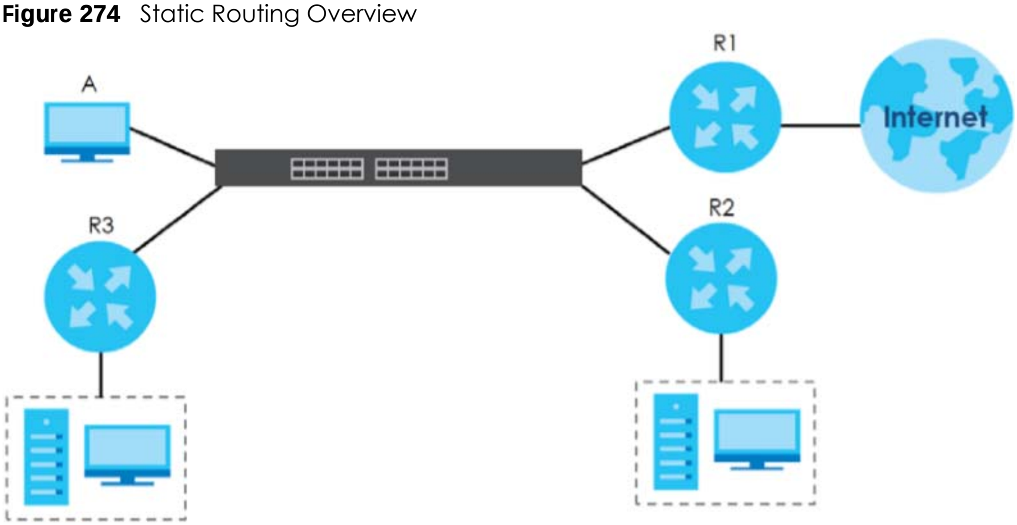
This chapter shows you how to configure static routes.

The Switch uses IP for communication with management computers, for example using HTTP, Telnet, SSH, or SNMP. Use IP static routes to have the Switch respond to remote management stations that are not reachable through the default gateway. The Switch can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

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 274 Static Routing Overview



42.1.1 What You Can Do

- Use the **Static Routing** screen (Section 42.2 on page 369) to display the link to the **IPv4 Static Route** screen.
- Use the **IPv4 Static Route** screen (Section 42.3 on page 369) to configure and enable an IPv4 static route.

42.2 Static Routing

Click **IP Application** > **Static Routing** in the navigation panel to display the screen as shown.

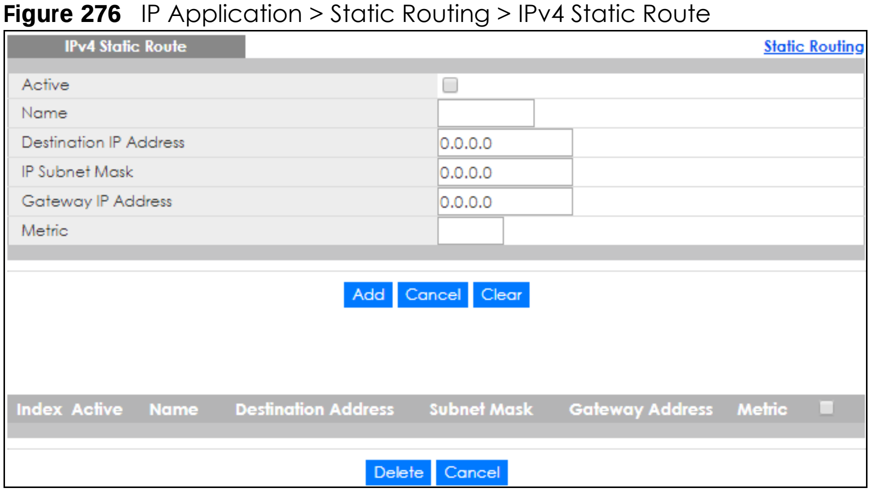
Click the link next to **IPv4 Static Route** to open a screen where you can create IPv4 static routing rules.

Figure 275 IP Application > Static Routing

42.3 IPv4 Static Route

Click the link next to **IPv4 Static Route** in the **IP Application** > **Static Routing** screen to display the screen as shown.

Figure 276 IP Application > Static Routing > IPv4 Static Route



The following table describes the related labels you use to create a static route.

Table 185 IP Application > Static Routing > IPv4 Static Route

LABEL	DESCRIPTION
Active	This field allows you to activate or deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **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 reset the above 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 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 an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
	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.

CHAPTER 43 Differentiated Services

43.1 DiffServ Overview

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

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.

43.1.1 What You Can Do

- Use the **DiffServ** screen (Section 43.2 on page 372) to activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.
- Use the **DSCP Setting** screen (Section 43.3.1 on page 373) to change the DSCP-IEEE 802.1p mapping.

43.1.2 What You Need to Know

Read on for concepts on Differentiated Services that can help you configure the screens in this chapter.

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 277 DiffServ: Differentiated Service Field

DSCP (6 bits)	CU (2 bits)

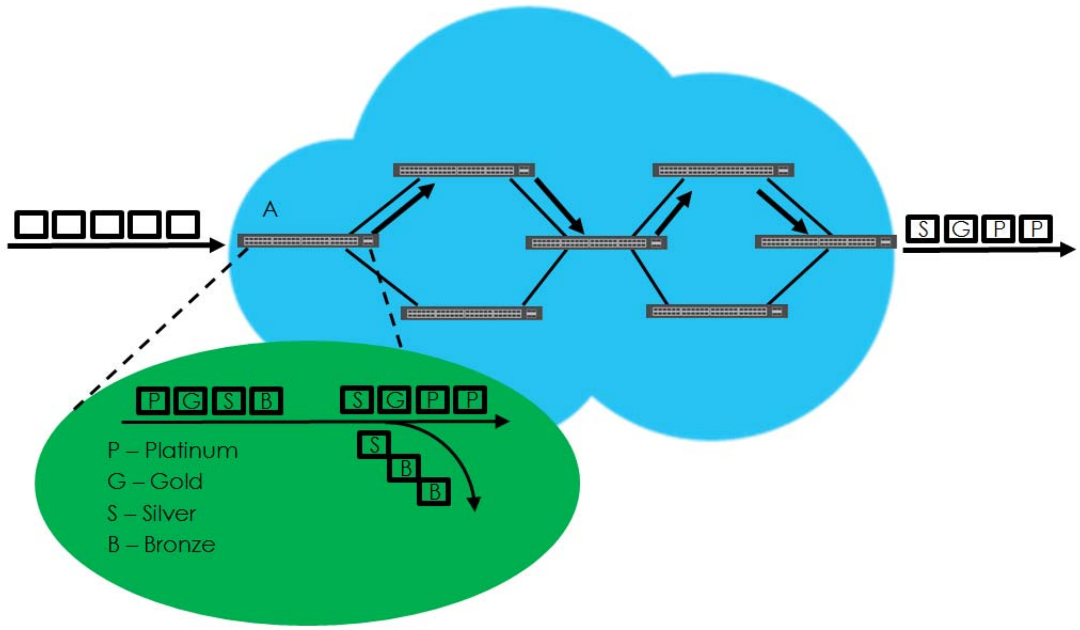
DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

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.

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 278) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 278 DiffServ Network

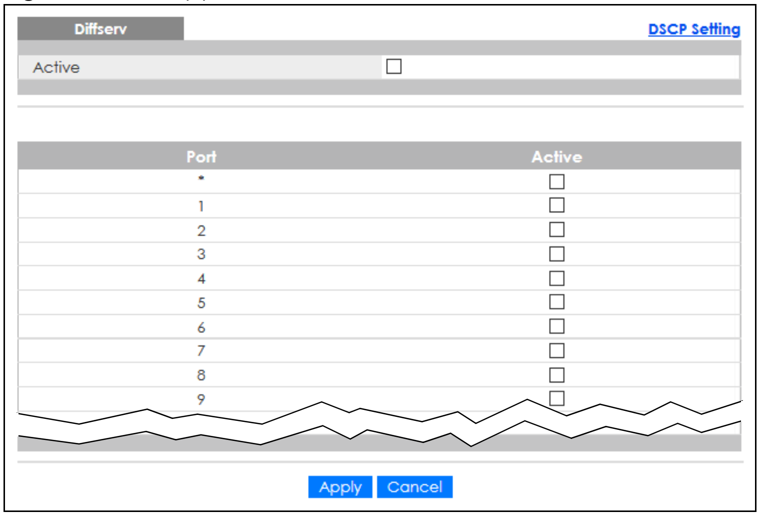


43.2 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected ports.

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 279 IP Application > DiffServ



The following table describes the labels in this screen.

Table 186 IP Application > DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. 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.

43.3 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.

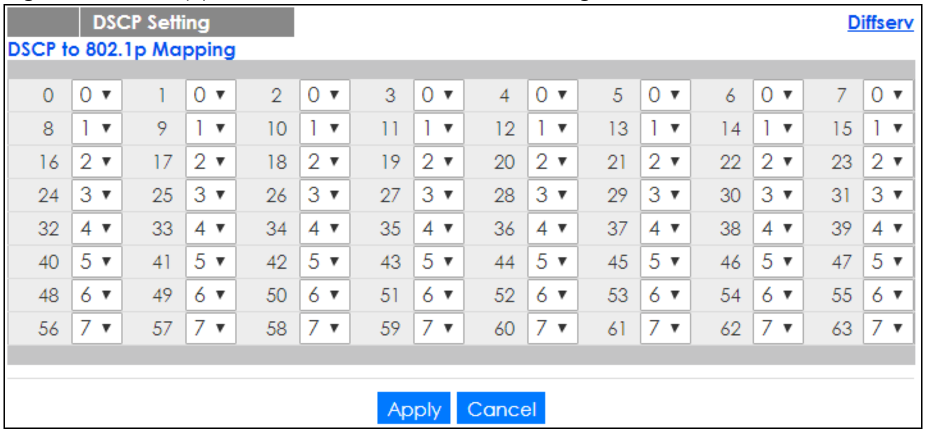
Table 187 Default DSCP-IEEE 802.1p Mapping

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

43.3.1 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 280 IP Application > DiffServ > DSCP Setting



The following table describes the labels in this screen.

Table 188 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.

CHAPTER 44
DHCP

44.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. If you configure the Switch as a DHCP relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you do not configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

44.1.1 What You Can Do

- Use the **DHCPv4 Status** screen (Section 44.3 on page 376) to display the relay mode.
- Use the **DHCPv4 Option 82 Profile** screen (Section 44.4.2 on page 378) to create DHCPv4 option 82 profiles.
- Use the **DHCPv4 Global Relay** screen (Section 44.4.3 on page 379) to configure global DHCPv4 relay.
- Use the **DHCPv4 Global Relay Port** screen (Section 44.4.4 on page 380) to apply a different DHCP option 82 profile to certain ports on the Switch.
- Use the **VLAN Setting** screen (Section 44.4.6 on page 382) to configure your DHCPv4 settings based on the VLAN domain of the DHCPv4 clients.
- Use the **DHCPv4 VLAN Port** screen (Section 44.4.7 on page 383) to apply a different DHCP option 82 profile to certain ports in a VLAN.
- Use the **DHCPv6 Relay** screen (Section 44.6 on page 387) to enable and configure DHCPv6 relay.
- Use the **DHCP Server Guard** screen (Section 44.6 on page 387) to specify whether ports are trusted or untrusted ports for DHCP packets.

44.1.2 What You Need to Know

Read on for concepts on DHCP that can help you configure the screens in this chapter.

DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

DHCPv4 Configuration Options

The DHCPv4 configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** – The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** – The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

44.2 DHCP Configuration

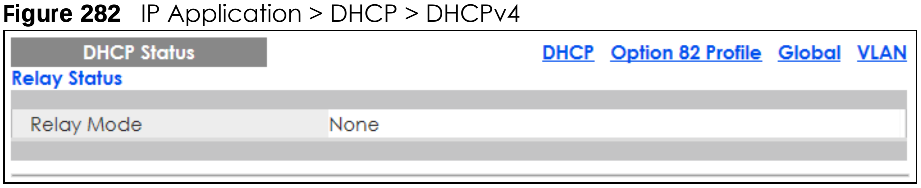
Click **IP Application** > **DHCP** in the navigation panel to display the screen as shown. Click the link next to **DHCPv4** to open screens where you can enable and configure DHCPv4 relay settings and create option 82 profiles. Click the link next to **DHCPv6** to open a screen where you can configure DHCPv6 relay settings. Click the link next to **DHCP Server Guard** to open a screen where you can specify whether ports are trusted or untrusted ports for DHCP packets.

Figure 281 IP Application > DHCP

44.3 DHCPv4 Status

Click **IP Application** > **DHCP** > **DHCPv4** in the navigation panel. The **DHCP Status** screen displays.

Figure 282 IP Application > DHCP > DHCPv4



The following table describes the labels in this screen.

Table 189 IP Application > DHCP > DHCPv4

LABEL	DESCRIPTION
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 VLANs.

44.4 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.

44.4.1 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.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Setting** > **General Setup**.

The following describes the DHCP relay agent information that the Switch sends to the DHCP server:

Table 190 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in **Basic Settings** > **General Setup**.

44.4.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 191 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.

44.4.1.2 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 192 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 193 DHCP Relay Agent Remote ID Sub-option Format

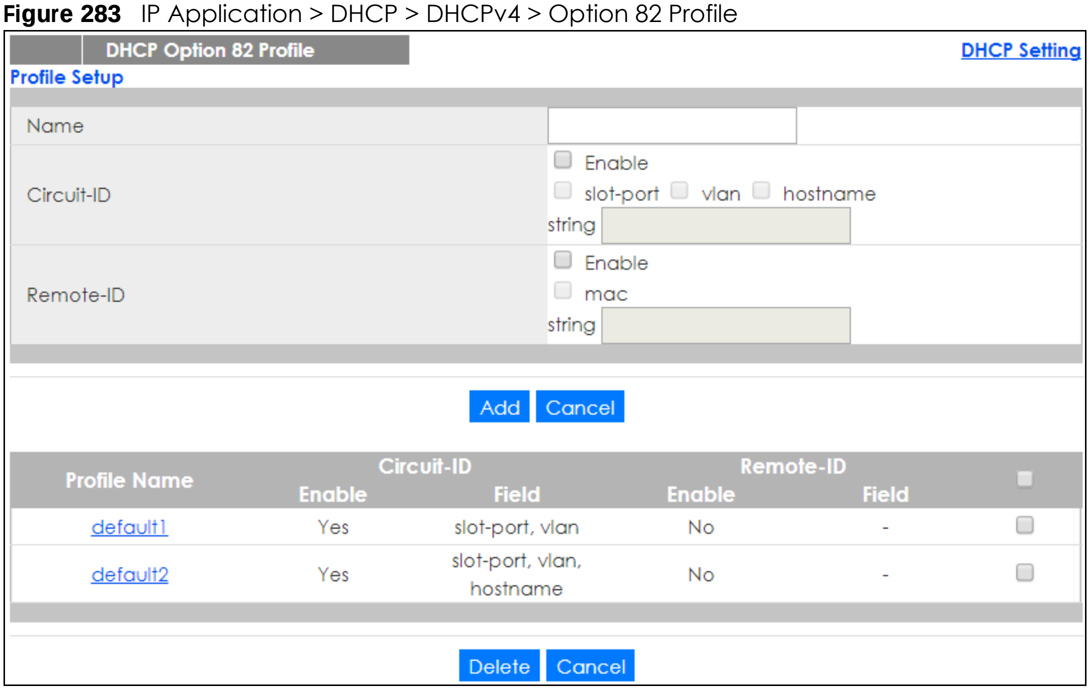
SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	MAC Address or String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and two identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

44.4.2 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 283 IP Application > DHCP > DHCPv4 > Option 82 Profile



The following table describes the labels in this screen.

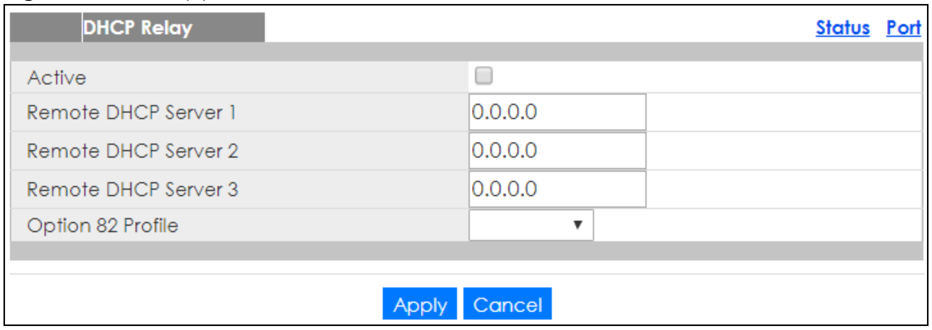
Table 194 IP Application > DHCP > DHCPv4 > Option 82 Profile

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.
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 entries that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

44.4.3 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 284 IP Application > DHCP > DHCPv4 > Global



The following table describes the labels in this screen.

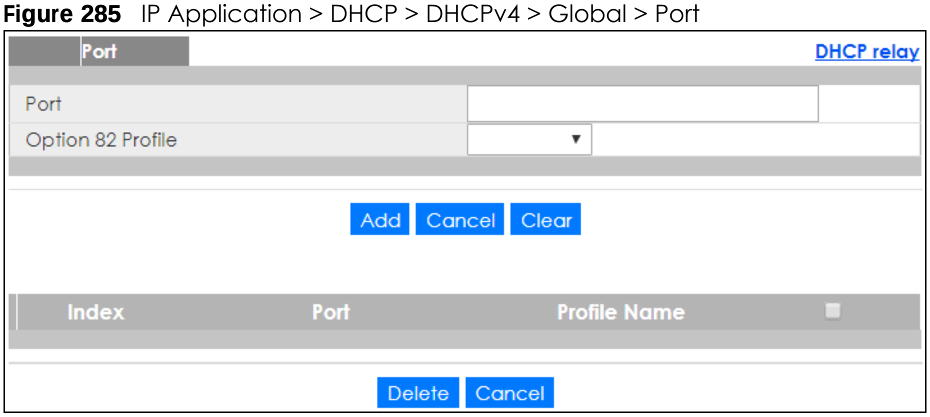
Table 195 IP Application > DHCP > DHCPv4 > Global

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.

44.4.4 Configure DHCPv4 Global Relay Port

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 285 IP Application > DHCP > DHCPv4 > Global > Port



The following table describes the labels in this screen.

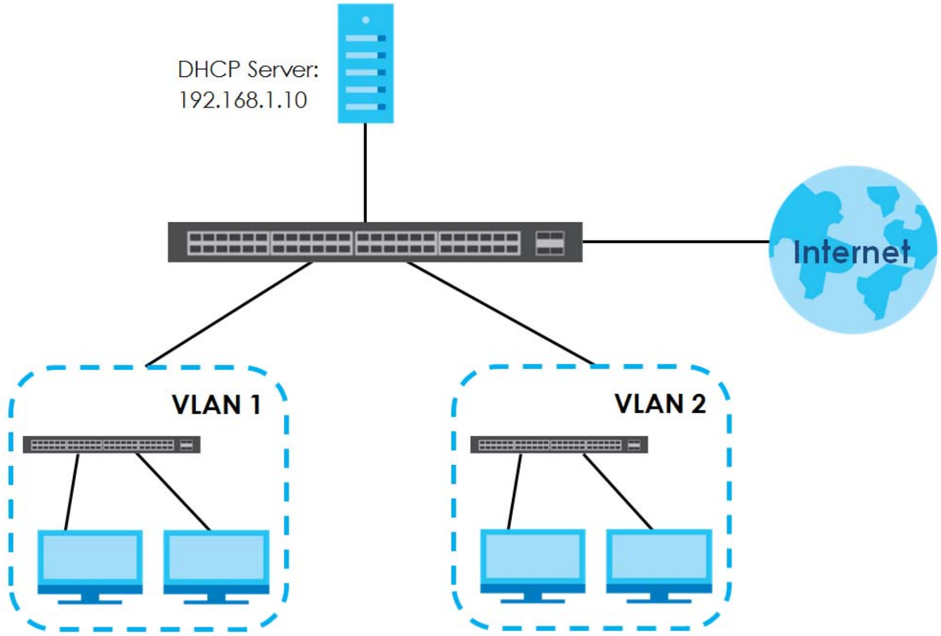
Table 196 IP Application > DHCP > DHCPv4 > Global > Port

LABEL	DESCRIPTION
Port	Enter the number of ports 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 example, enter “3–5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified 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. 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 ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports.
	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 entries that you want to remove, then click the **Delete** button to remove the selected entries from the table.
Cancel	Click this to clear the check boxes above.

44.4.5 Global DHCP Relay Configuration Example

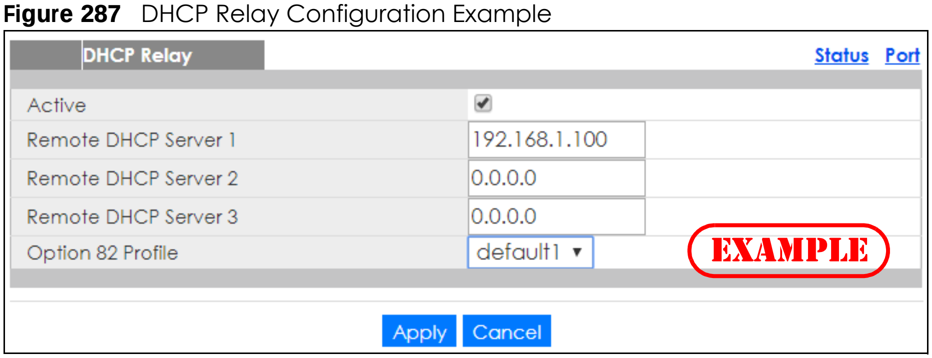
The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 286 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 287 DHCP Relay Configuration Example

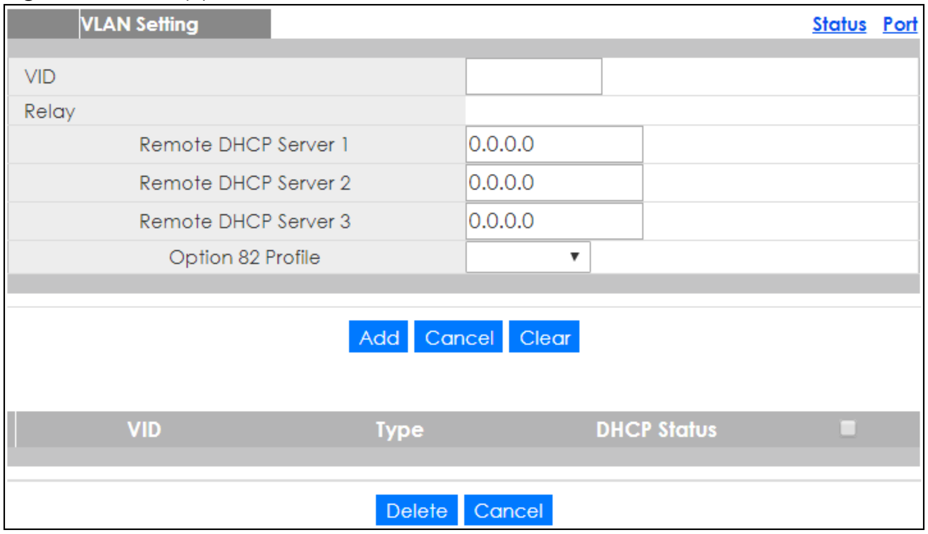


44.4.6 DHCPv4 VLAN Setting

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 5.1.3 on page 81 for information on how to do this.

Figure 288 IP Application > DHCP > DHCPv4 > VLAN



The following table describes the labels in this screen.

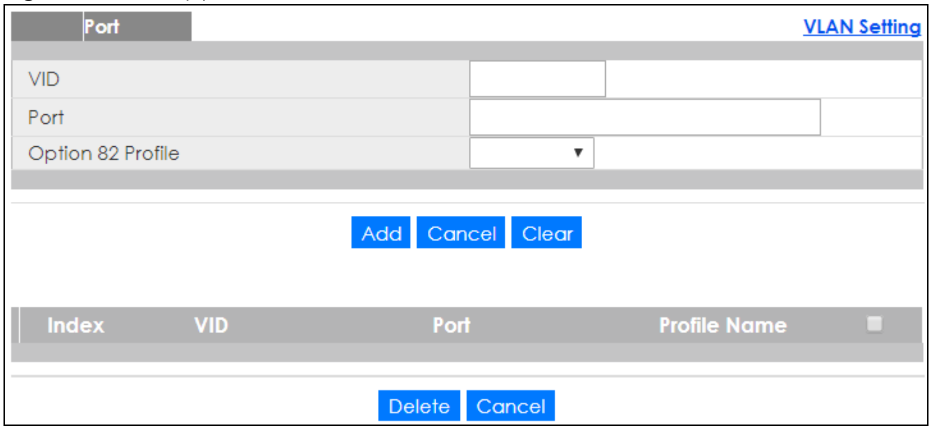
Table 197 IP Application > DHCP > DHCPv4 > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
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 **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.

44.4.7 Configure DHCPv4 VLAN Port

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 289 IP Application > DHCP > DHCPv4 > VLAN > Port



The following table describes the labels in this screen.

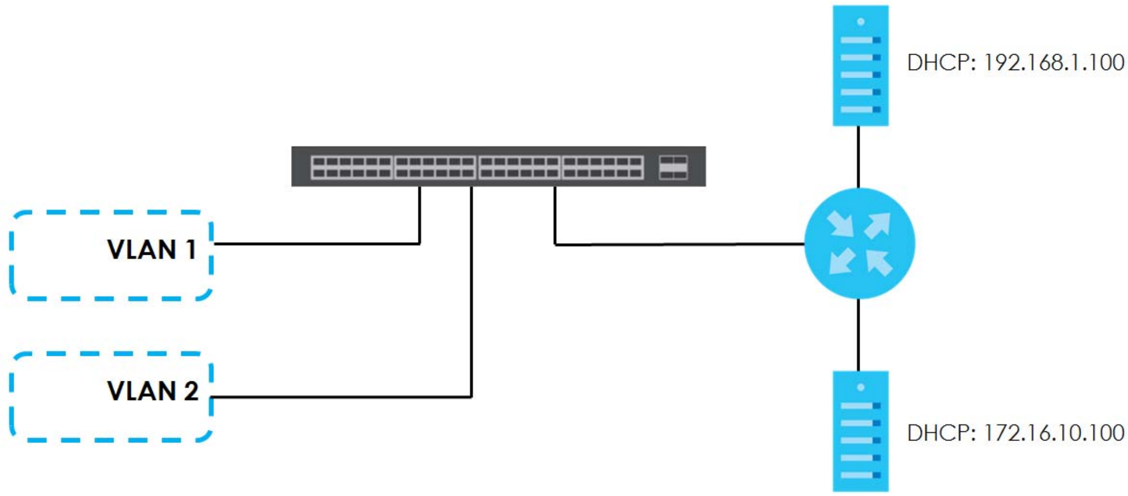
Table 198 IP Application > DHCP > DHCPv4 > VLAN > Port

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of ports 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 example, enter "3–5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified 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. 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 ports belongs.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports 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 entries that you want to remove, then click the **Delete** button to remove the selected entries from the table.
Cancel	Click this to clear the check boxes above.

44.4.8 Example: DHCP Relay for Two VLANs

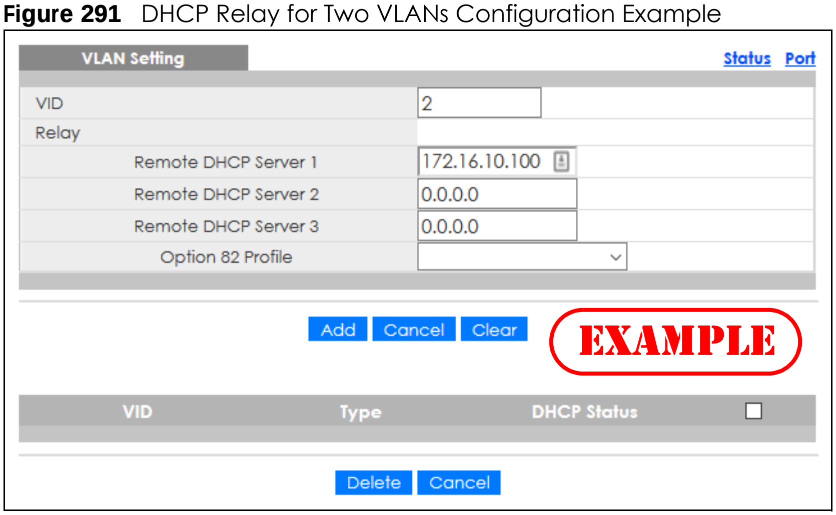
The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.16.10.100.

Figure 290 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 291 DHCP Relay for Two VLANs Configuration Example



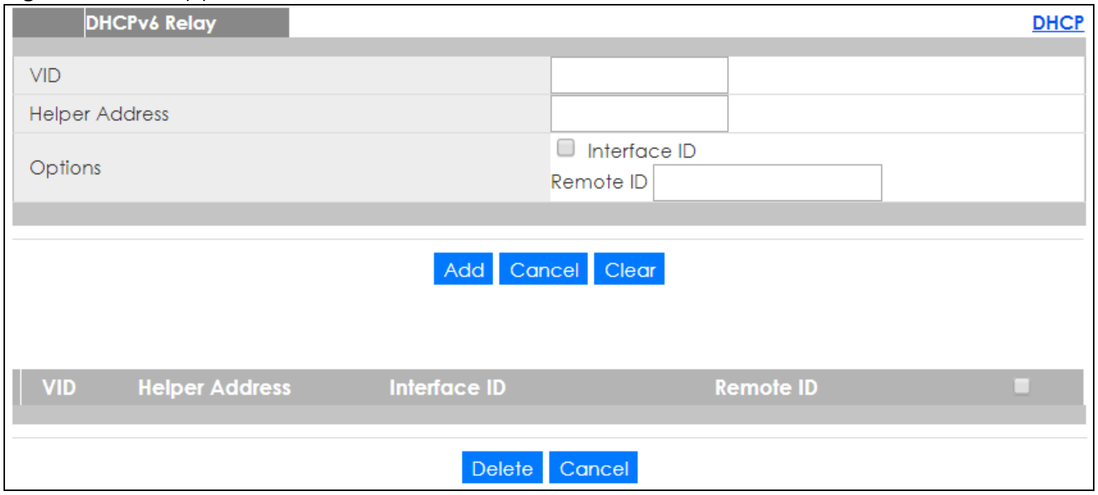
44.5 DHCPv6 Relay

A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCPv6 server on its network, it then needs a DHCPv6 relay agent to send a message to a DHCPv6 server that is not attached to the same network.

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 292 IP Application > DHCP > DHCPv6



The following table describes the labels in this screen.

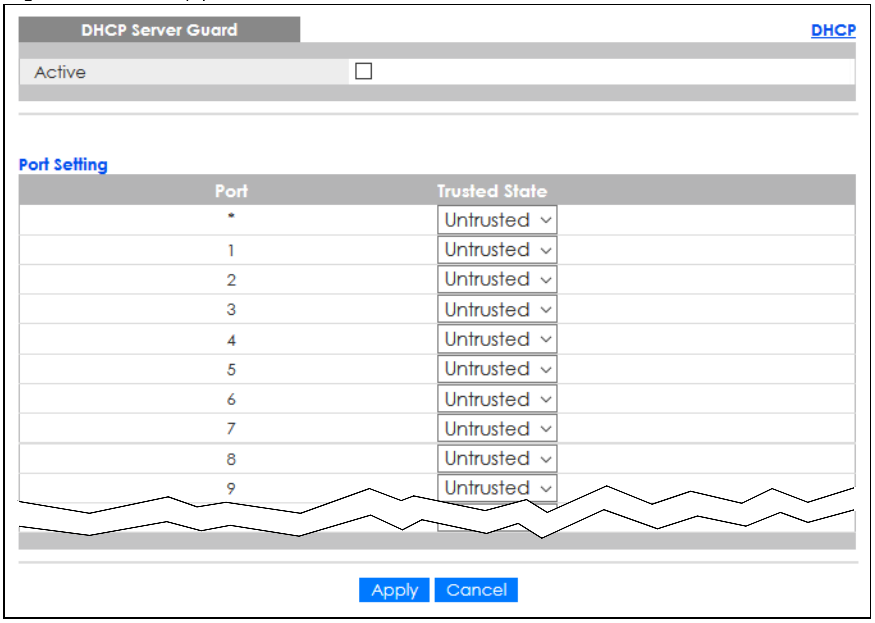
Table 199 IP Application > DHCP > DHCPv6

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Helper Address	Enter the remote DHCPv6 server address for the specified VLAN.
Options	
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 entries that you want to remove and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes.

44.6 DHCP Server Guard

Use this screen to specify whether ports are trusted or untrusted ports for DHCP packets. Click **IP Application** > **DHCP** > **DHCP Server Guard** in the navigation panel to display the screen as shown.

Figure 293 IP Application > DHCP > DHCP Server Guard



The following table describes the labels in this screen.

Table 200 IP Application > DHCP > DHCP Server Guard

LABEL	DESCRIPTION
Active	Select this option to enable DHCP Server Guard.
Port Setting	
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). The Switch does not discard DHCP packets on trusted ports for any reason. The Switch discards DHCP packets from untrusted ports when the packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
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 their last saved values.

CHAPTER 45
ARP Setup

45.1 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.

45.1.1 What You Can Do

- Use the **ARP Learning** screen (Section 45.2.1 on page 390) to configure ARP learning mode on a per-port basis.

45.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

45.1.2.1 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.

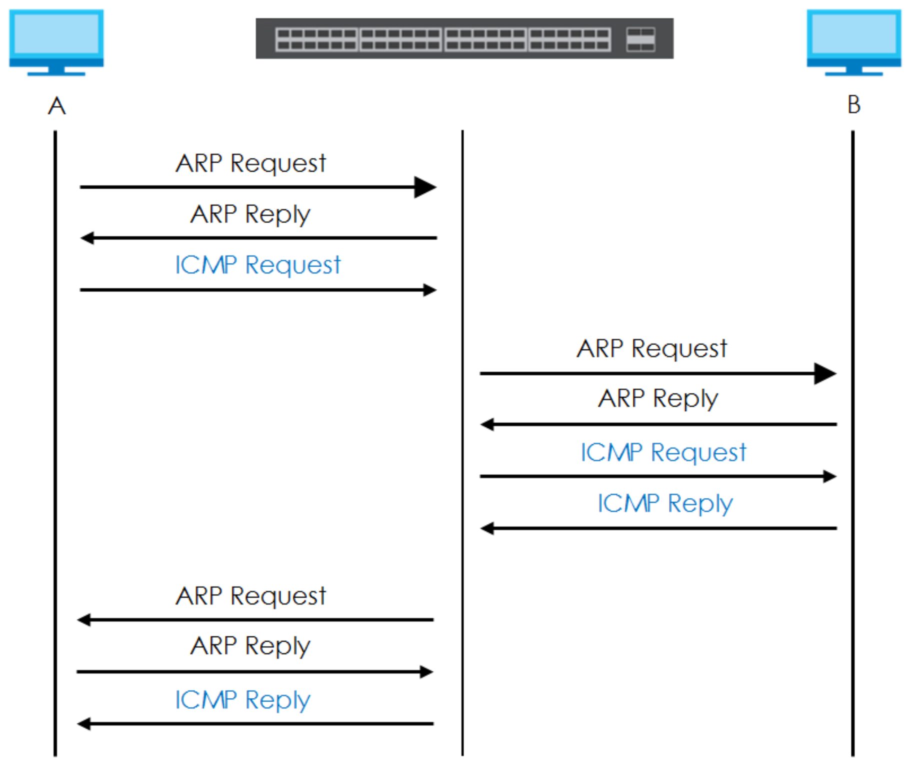
45.1.2.2 ARP Learning Mode

The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

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**.



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.

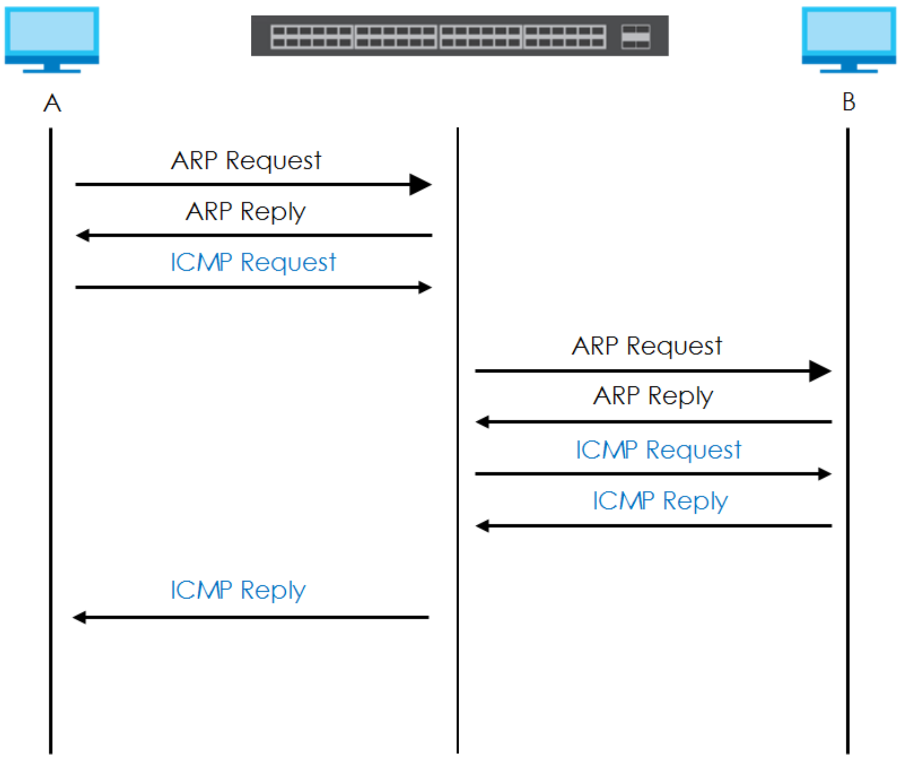
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

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.

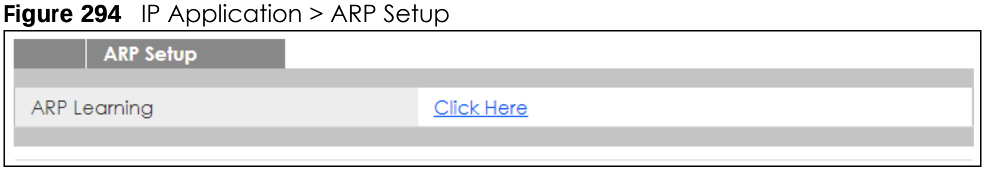
Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



45.2 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.

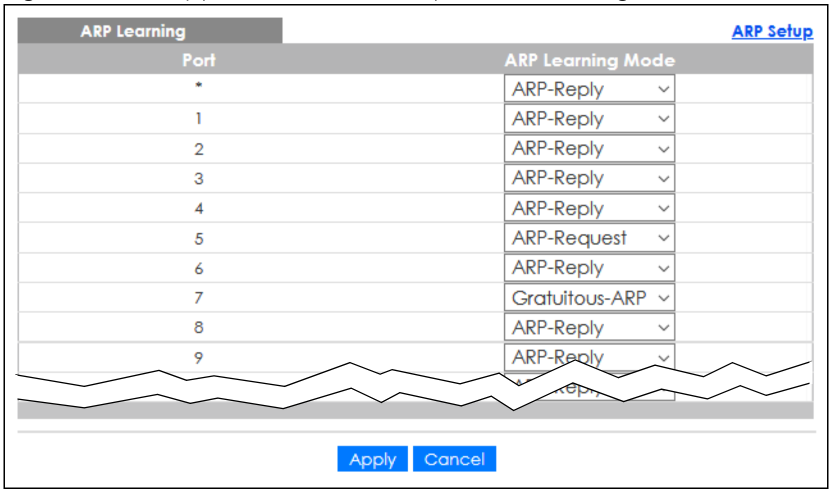
Figure 294 IP Application > ARP Setup



45.2.1 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 295 IP Application > ARP Setup > ARP Learning



The following table describes the labels in this screen.

Table 201 IP Application > ARP Setup > ARP Learning

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. 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.

CHAPTER 46
Maintenance

46.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

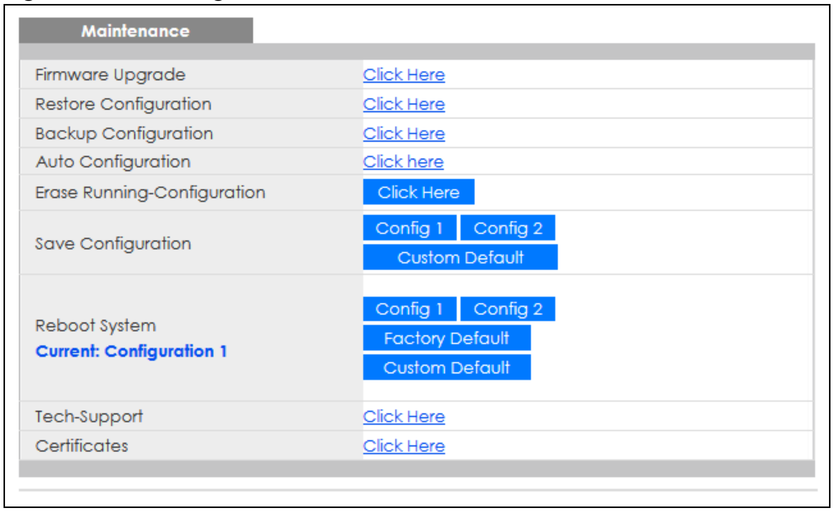
46.1.1 What You Can Do

- Use the **Maintenance** screen (Section 46.2 on page 392) to manage firmware and your configuration files.
- Use the **Firmware Upgrade** screen (Section 46.3 on page 396) to upload the latest firmware.
- Use the **Restore Configuration** screen (Section 46.4 on page 397) to upload a stored device configuration file.
- Use the **Backup Configuration** screen (Section 46.5 on page 398) to save your configurations for later use.
- Use the **Auto Configuration** screen (Section 46.6 on page 398) to overwrite the running configuration stored in the Switch's RAM.
- Use the **Erase Running-Configuration** screen (Section 46.2.1 on page 394) to reset the configuration to the Zyxel default configuration settings.
- Use the **Save Configuration** screen (Section 46.2.2 on page 394) to save the current configuration settings to a specific configuration file on the Switch.
- Use the **Reboot System** screen (Section 46.2.3 on page 394) to restart the Switch without physically turning the power off and load a specific configuration file.
- Use the **Tech-Support** screen (Section 46.7 on page 399) to create reports for customer support if there are problems with the Switch.
- Use the **Certificates** screen (Section 46.8 on page 401) to see the **Certificate** screen and import the Switch's CA-signed certificates.

46.2 Maintenance Settings

Use this screen to manage firmware and your configuration files. Click **Management** > **Maintenance** in the navigation panel to open the following screen.

Figure 296 Management > Maintenance



The following table describes the labels in this screen.

Table 202 Management > Maintenance

LABEL	DESCRIPTION
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.
Auto Configuration	Click **Click Here** to go to the **Auto Configuration** screen.
Erase Running-Configuration	Click **Click Here** to reset the configuration to the Zyxel default configuration 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. Click **Custom Default** to save the current configuration settings to a customized default file on the Switch. This file can be used instead of the Zyxel factory default configuration file.
Reboot System	Click **Config 1** to reboot the Switch and load **Configuration 1** on the Switch. Click **Config 2** to reboot the Switch and load **Configuration 2** on the Switch. Click **Factory Default** to reboot the Switch and load the Zyxel factory default configuration settings on the Switch. Click **Custom Default** to reboot the Switch and load a saved customized default file 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.
Current	This field displays which configuration (**Configuration 1** or **Configuration 2**) is currently operating 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.
Certificates	Click **Click Here** to see the **Certificate** screen and import the Switch's CA-signed certificates.

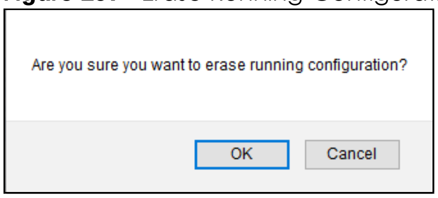
46.2.1 Erase Running-Configuration

Follow the steps below to clear current configuration on the Switch. This will reset the Switch back to its factory defaults. Or, click the **Factory Default** button in **Reboot System**.

1 In the **Maintenance** screen, click the **Click Here** button next to **Erase Running-Configuration** to clear all Switch configuration information you configured and return to the Zyxel default configuration settings.

2 Click **OK** to reset all Switch configurations to the Zyxel default configuration settings.

Figure 297 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 or DHCP-assigned IP).

46.2.2 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch. These configurations are set up according to your network environment.

Click **Config 2** to save the current configuration settings permanently to **Configuration 2** on the Switch. These configurations are set up according to your network environment.

Click **Custom Default** to save the current configuration settings permanently to a customized default file on the Switch. If configuration changes cause the Switch to behave abnormally, click **Custom Default** (next to **Reboot System**) to have the Switch automatically reboot and restore the saved **Custom Default** configuration file.

Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration 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.

46.2.3 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**), a **Custom Default** or the **Factory Default** configuration when you reboot. Follow the steps below to reboot the Switch.

1 In the **Maintenance** screen, click a configuration button next to **Reboot System** to reboot and load that configuration file. The confirmation screen displays.

2 Click **OK** again and then wait for the Switch to restart. This takes up to 2 minutes. This does not affect the Switch's configuration.

Click **Config 1** and follow steps 1 to 2 to reboot and load configuration one on the Switch.

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 Zyxel factory default configuration settings on the Switch.

Click **Custom Default** and follow steps 1 to 2 to reboot and load a customized default file on the Switch. This will save the custom default configuration settings to both **Configuration 1** and **Configuration 2**.

Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration on the Switch.

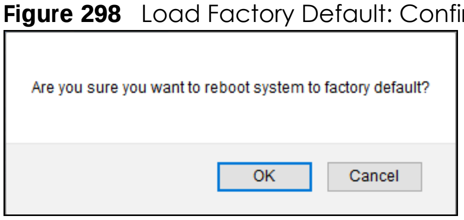
46.2.4 Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

1 Click the **Factory Default** button.

2 Click **OK** to continue or **Cancel** to abort.

Figure 298 Load Factory Default: Confirmation



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 or DHCP-assigned IP).

46.2.5 Custom Default

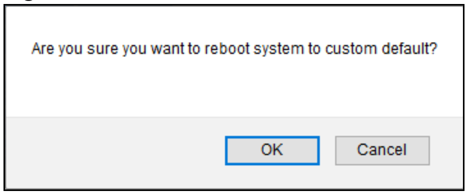
Follow the steps below to reset the Switch back to the **Custom Default** configuration file you created. This will save the custom default configuration settings to both **Configuration 1** and **Configuration 2**.

1 Click the **Custom Default** button.

2 Click **OK** to continue or **Cancel** to abort.

Note: If you did not save a custom default file in the Web Configurator, then the factory default file is restored after you press click **Custom Default** (next to **Reboot System**) on the Switch. You will then have to make all your configurations again on the Switch.

Figure 299 Load Custom Default: Confirmation



46.3 Firmware Upgrade

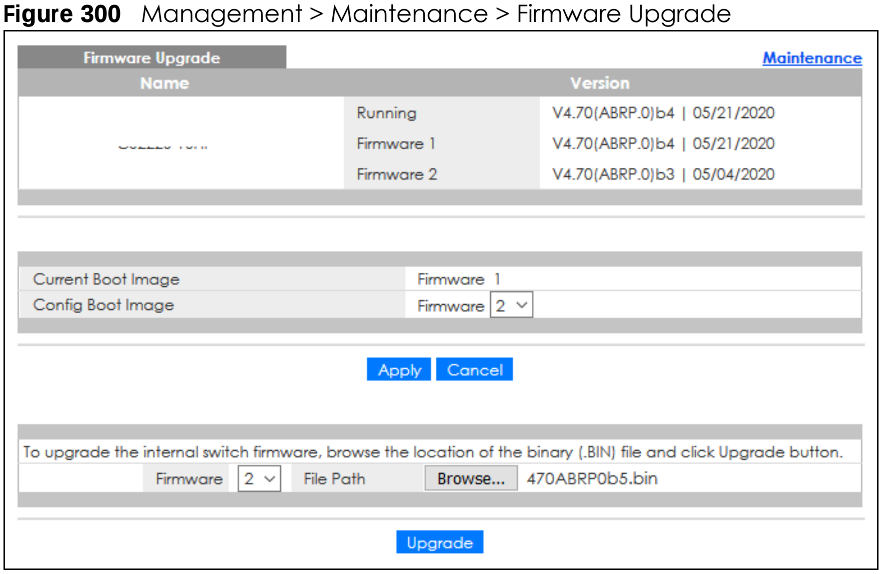
Use the following screen to upgrade your Switch to the latest firmware. The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the Web Configurator and to specify which image is loaded when the Switch starts up.

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.

Click **Management** > **Maintenance** > **Firmware Upgrade** to view the screen as shown next.

Figure 300 Management > Maintenance > Firmware Upgrade



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 **Choose File** or **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 process is complete, see the **System Info** screen to verify your current firmware version number.

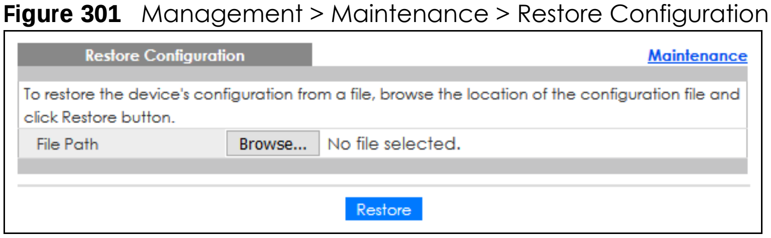
Table 203 Management > Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Name	This is the name of the Switch that you are configuring.
Version	The Switch has 2 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, click **Apply** and reboot the Switch to see changes, you will also see changes in the **Current Boot Image** field above as well.
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.
	This field appears only in 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**.
File Path	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 **Choose File** or **Browse** to locate it.
Upgrade	Click **Upgrade** to load the new firmware. s are only applied after a reboot. To reboot, go to **Management** > **Maintenance** > **Reboot System** and 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).

46.4 Restore Configuration

Use this screen to restore a previously saved configuration from your computer to the Switch.

Figure 301 Management > Maintenance > Restore Configuration



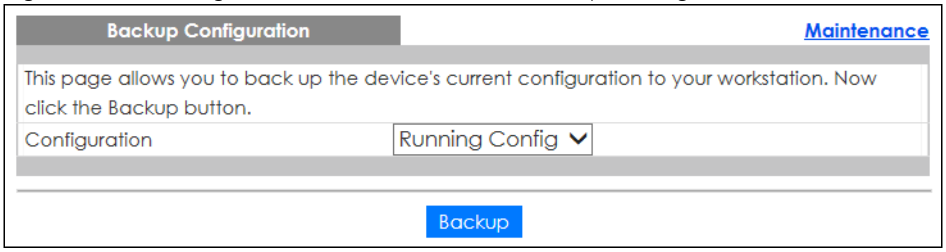
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Choose File** or **Browse** to locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

46.5 Backup Configuration

Backing up your Switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 302 Management > Maintenance > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Select which Switch configuration file you want to download to your computer.

2 Click **Backup**.

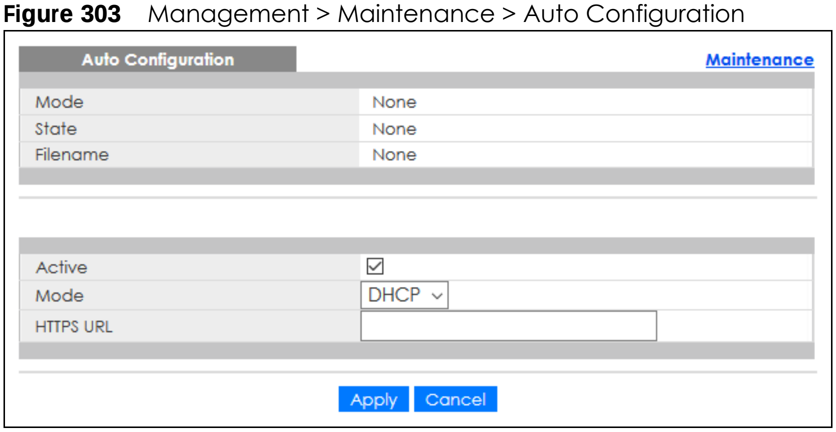
3 If the current configuration file is open and/or downloaded to your computer automatically, you can click **File** > **Save As** to save the file to a specific place.

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.

46.6 Auto Configuration

The Switch can download an pre-saved auto configuration file automatically when you reboot the Switch using the DHCP or HTTPS mode. This will overwrite the running configuration stored in the Switch's RAM instead of the startup configuration stored in the Switch's flash memory.

Figure 303 Management > Maintenance > Auto Configuration



The following table describes the labels in this screen.

Table 204 Management > Maintenance > Auto Configuration

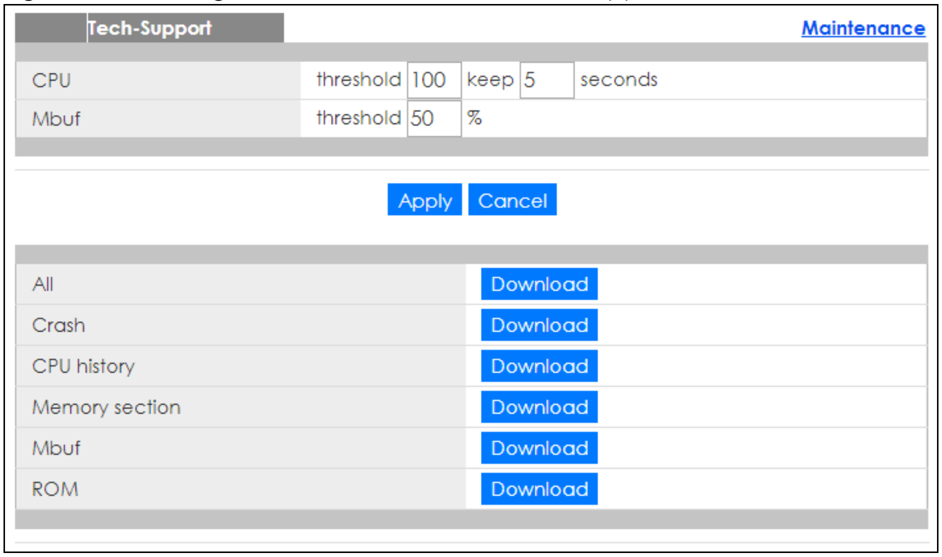
LABEL	DESCRIPTION
Use this section to view the auto configuration status after you restarted the Switch.	
Mode	This field shows the mode (**DHCP** or **HTTPS**) that is used for auto configuration after you enabled auto configuration and restarted the Switch. It shows **None** if auto configuration was not enabled.
State	This field shows whether auto configuration was executed successfully the last time the Switch rebooted. **None** – Auto configuration was disabled and not executed. **Success** – An auto configuration file was downloaded successfully to the Switch. **Un-success** – An auto configuration file was not downloaded to the Switch.
Filename	This field displays the name of the auto configuration file that was downloaded the last time the Switch rebooted. It shows **None** if auto configuration was not enabled or not executed successfully.
Use this section to enable auto configuration and select the mode that you want to use for auto configuration.	
Active	Select the check box to enable auto configuration.
Mode	Select **DHCP** to have the Switch use the TFTP server IP address and auto configuration file name assigned by a DHCP server to download a pre-saved configuration file when the Switch reboots. Note: The Switch should act as a DHCP client to send a DHCP request so that it can get the TFTP server address and configuration file name from the DHCP server. Select **HTTPS** to have the Switch use the URL you specified in the **HTTPS URL** field to access a web server and download the auto configuration file using HTTPS.
HTTPS URL	Type the URL that can be used to access and download the auto configuration file from a web server using HTTPS. For example, https://webserverIPaddress/configfilename.cfg. Note: You must fill in this field if you select **HTTPS** in the **Mode** field. Otherwise, auto configuration will not work.
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.

46.7 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 **Management** > **Maintenance** > **Tech-Support** to see the following screen.

Figure 304 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 205 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 and 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 when the Switch is shutdown or during power outage.
Memory Section	Click **Download** to see the memory section log report. This log report is stored in flash memory.

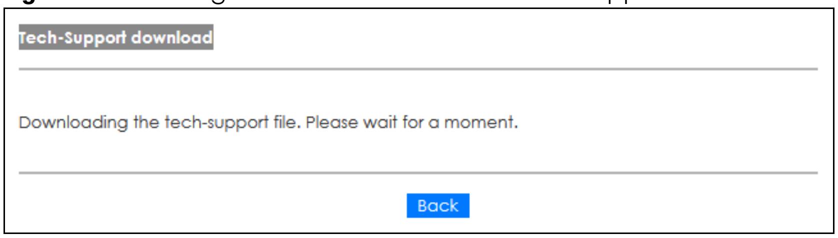
Table 205 Management > Maintenance > Tech-Support (continued)

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.

46.7.1 Tech-Support Download

When you click **Download** to save your current Switch configuration to a computer, the following screen appears. When the log report has downloaded successfully, click **Back** to return to the previous screen.

Figure 305 Management > Maintenance > Tech-Support: Download



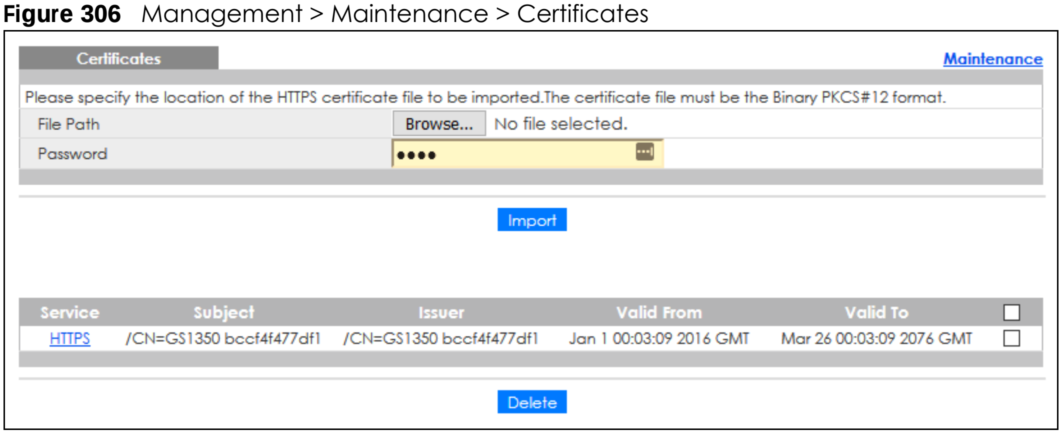
46.8 Certificates

The Switch can use HTTPS certificates that are verified by a third party to create secure HTTPS connections between your computer and the Switch. This way, you may securely access the Switch using the Web Configurator. See Section 47.7.3 on page 424 for more information about HTTPS.

Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Click **Management** > **Maintenance** > **Certificates** to open the following screen. Use this screen to import the Switch's CA-signed certificates.

Figure 306 Management > Maintenance > Certificates



The following table describes the labels in this screen.

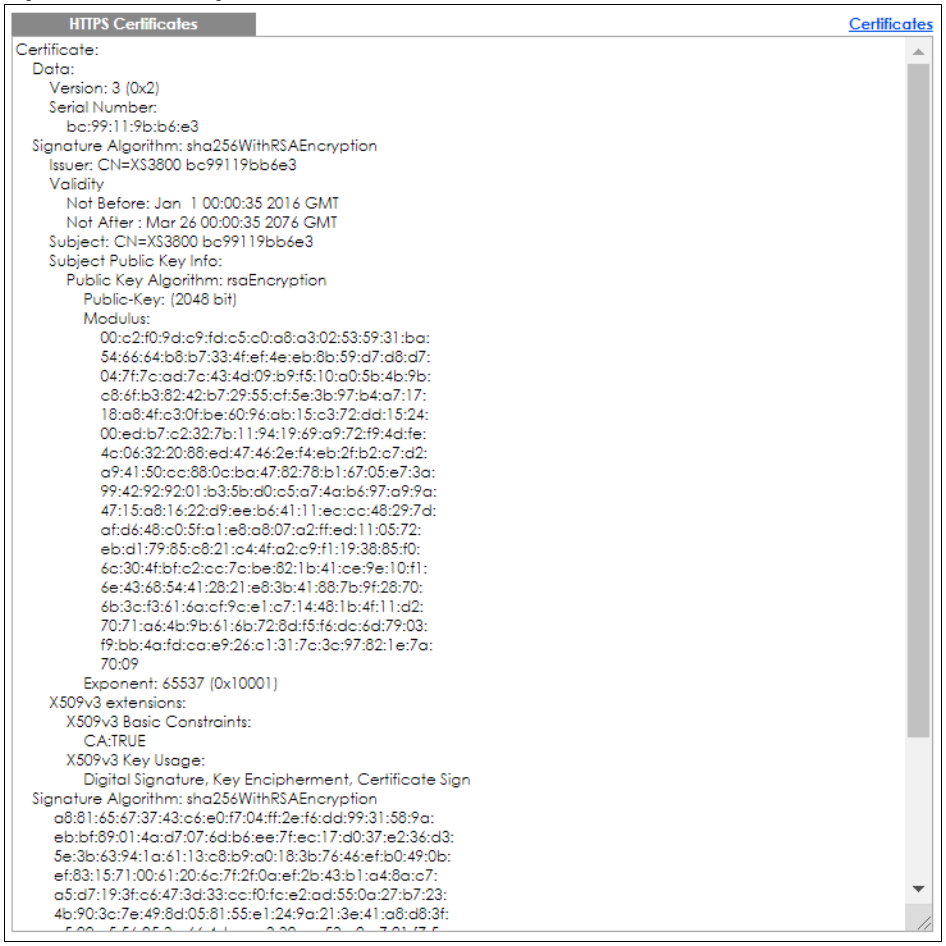
Table 206 Management > Maintenance > Certificates

LABEL	DESCRIPTION
File Path	Click **Choose File** or **Browse** to find the certificate file you want to upload.
Password	Type the certificate file's password that was created when the PKCS #12 file was exported. The password consists of up to 32 ASCII characters.
Import	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Switch.
Service	This field displays the service type that this certificate is for.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires.
	Select an entry's check box to select a specific entry.
Delete	Click this button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

46.8.1 HTTPS Certificates

Use this screen to view the HTTPS certificate details. Click a hyperlink in the **Service** column in the **Management** > **Maintenance** > **Certificates** screen to open the following screen.

Figure 307 Management > Maintenance > Certificates > HTTPS



46.9 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

46.9.1 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.

46.9.2 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the Zyxel factory default configuration 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 207 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.cfg	This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

46.9.2.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

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” and “ras”. 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.

46.9.3 FTP Command Line Procedure

1 Launch the FTP client on your computer.

2 Enter `open`, followed by a space and the IP address of your Switch.

3 Press **[ENTER]** when prompted for a username.

4 Enter your password as requested (the default is “1234”).

5 Enter `bin` to set transfer mode to binary.

6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to “ras”. 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 207 on page 404 for more information on filename conventions.

7 Enter `quit` to exit the ftp prompt.

46.9.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 208 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).

46.9.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP addresses 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.

CHAPTER 47 Access Control

47.1 Access Control Overview

This chapter describes how to control access to the Switch.

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 209 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to 9 sessions		One session	Up to 5 accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the CLI Reference Guide for more information on disabling multi-login.

47.1.1 What You Can Do

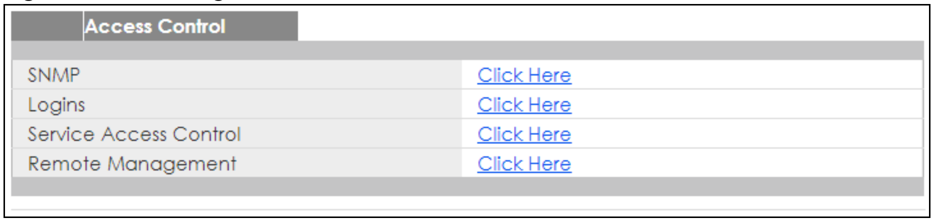
- Use the **Access Control** screen (Section 47.2 on page 406) to display the main screen.
- Use the **SNMP** screen (Section 47.3 on page 407) to configure your SNMP settings.
- Use the **Trap Group** screen (Section 47.3.1 on page 408) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **User Information** screen (Section 47.3.3 on page 410) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **Logins** screens (Section 47.4 on page 412) to assign which users can access the Switch via Web Configurator at any one time.
- Use the **Service Access Control** screen (Section 47.5 on page 414) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen (Section 47.6 on page 415) to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

47.2 Access Control Main Settings

Use this screen to display the main screen.

Click **Management** > **Access Control** in the navigation panel to display the main screen as shown.

Figure 308 Management > Access Control



The following table describes the labels in this screen.

Table 210 Management > Access Control

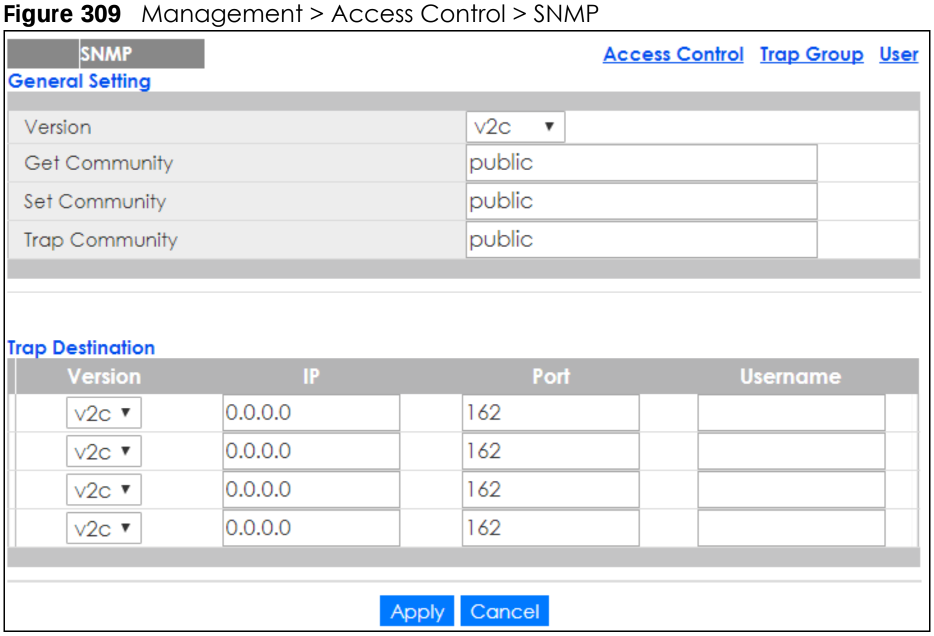
LABEL	DESCRIPTION
SNMP	Click this link to configure your SNMP settings.
Logins	Click this link to assign which users can access the Switch via Web Configurator at any one time.
Service Access Control	Click this link to decide what services you may use to access the Switch.
Remote Management	Click this link to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

47.3 Configure SNMP

Use this screen to configure your SNMP settings.

Click **Management** > **Access Control** > **SNMP** to view the screen as shown.

Figure 309 Management > Access Control > SNMP



The following table describes the labels in this screen.

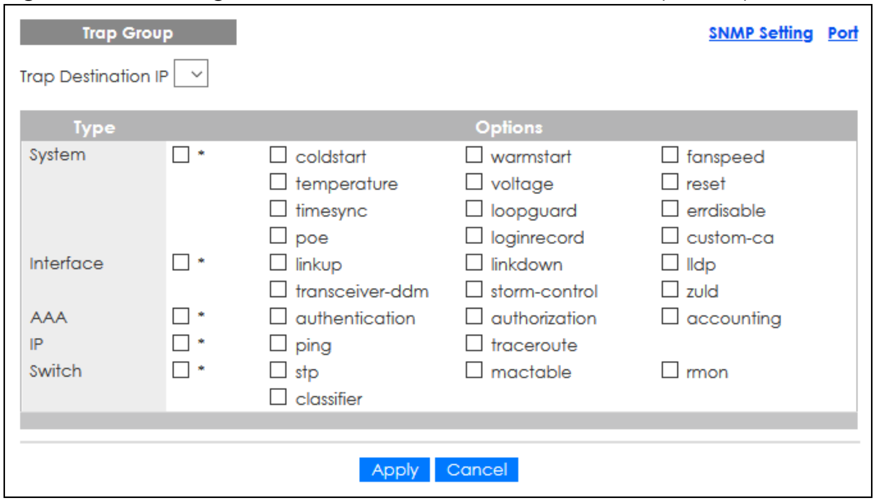
Table 211 Management > Access Control > SNMP

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**). 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**, which is the password for 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. 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.

47.3.1 Configure 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 310 Management > Access Control > SNMP > Trap Group



The following table describes the labels in this screen.

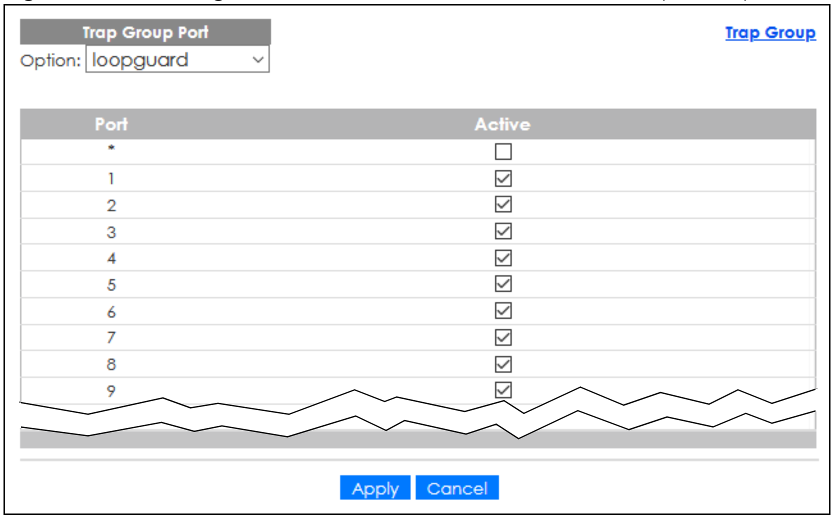
Table 212 Management > Access Control > SNMP > Trap Group

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. 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.

47.3.2 Enable or Disable 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 ports would be sent to the SNMP manager.

Figure 311 Management > Access Control > SNMP > Trap Group > Port



The following table describes the labels in this screen.

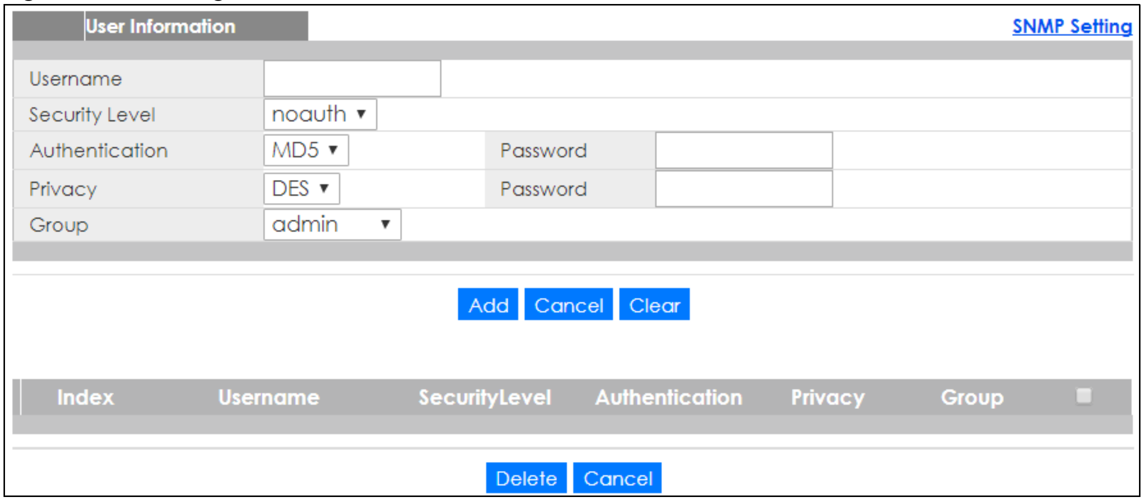
Table 213 Management > Access Control > SNMP > Trap Group > Port

LABEL	DESCRIPTION
Option	Select the trap type you want to configure here.
Port	This field displays a 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. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the trap type 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.

47.3.3 Configure 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 312 Management > Access Control > SNMP > User



The following table describes the labels in this screen.

Table 214 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.
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.

Table 214 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
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.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to begin configuring this screen afresh.

47.4 Set Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via Web Configurator at any one time.

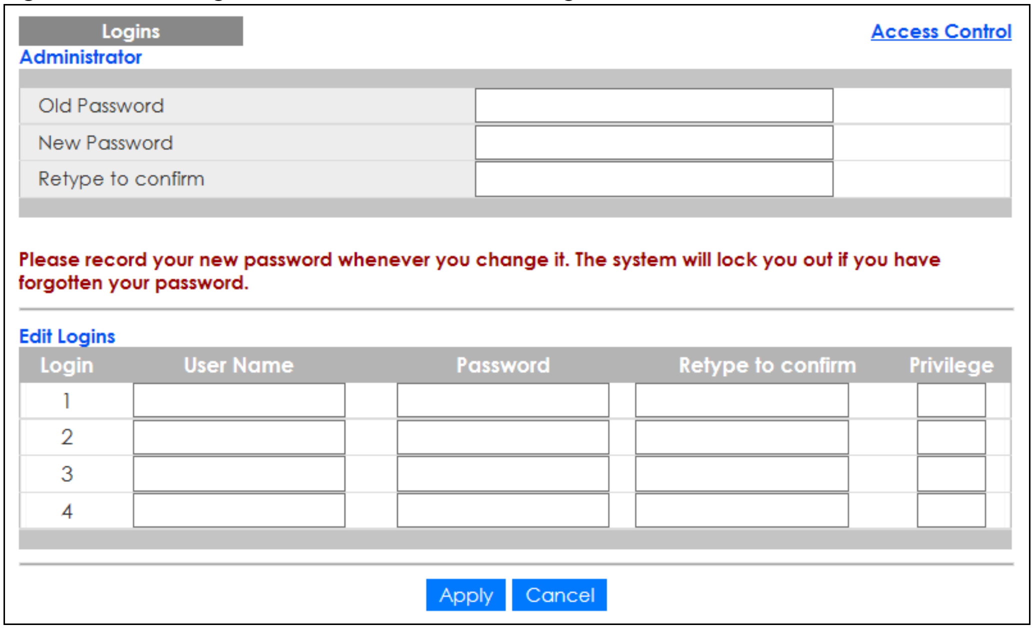
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

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 and/or configure Switch settings. The configuration right varies depending on the user's privilege level.

Click **Management** > **Access Control** > **Logins** to view the screen as shown.

Figure 313 Management > Access Control > Logins



The following table describes the labels in this screen.

Table 215 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.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation.
Edit Logins You may configure passwords for up to four users. These users can have read-only or read/write access. You can give users higher privileges via the Web Configurator or the CLI. For more information on assigning privileges via the CLI 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.

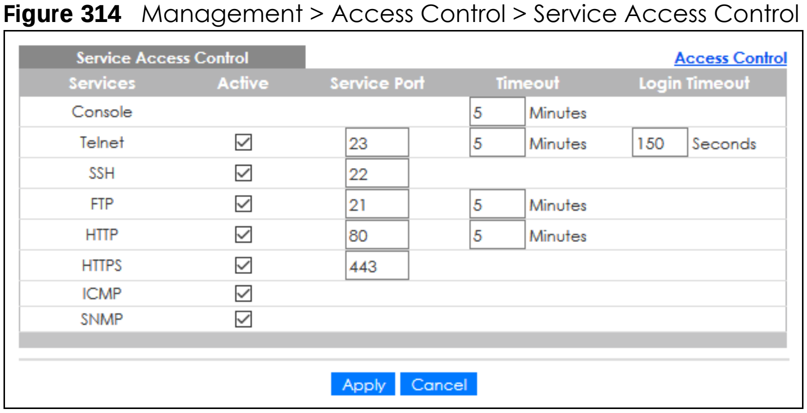
Table 215   Management > Access Control > Logins (continued)

LABEL	DESCRIPTION
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 or 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.

47.5 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 computers" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 314   Management > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 216   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.

Table 216   Management > Access Control > Service Access Control (continued)

LABEL	DESCRIPTION
Timeout	Enter 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.
Login Timeout	The Telnet or SSH server do not allow multiple user logins at the same time. Enter how many seconds (from 30 to 300 seconds) a login session times out. After it times out you have to start the login session again. Very long login session timeouts may have security risks. For example, if User A attempts to connect to the Switch (via SSH), but during the login stage, do not enter the user name and/or password, User B cannot connect to the Switch (via SSH) before the **Login Timeout** for User A expires (default 150 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.

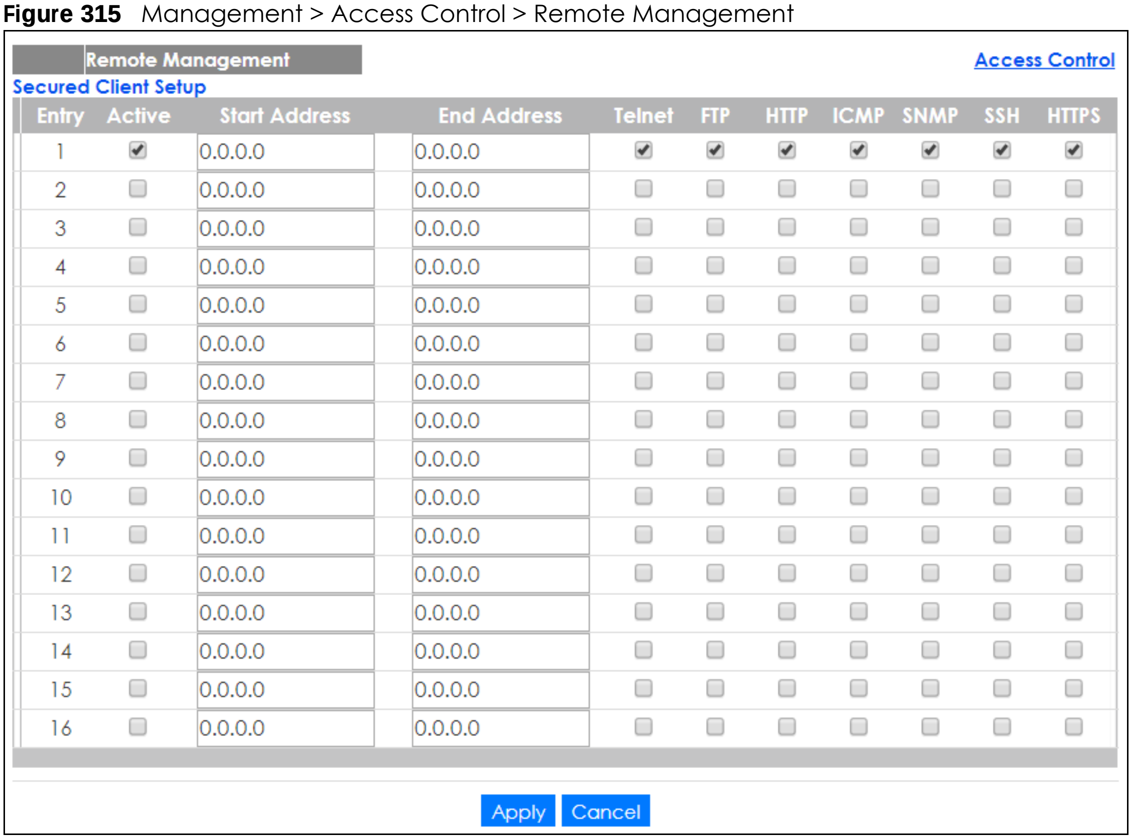
47.6 Remote Management

Use this screen to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

Click **Management** > **Access Control** > **Remote Management** to view the screen as shown next.

Click **Access Control** to return to the **Access Control** screen.

Figure 315   Management > Access Control > Remote Management



The following table describes the labels in this screen.

Table 217 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.

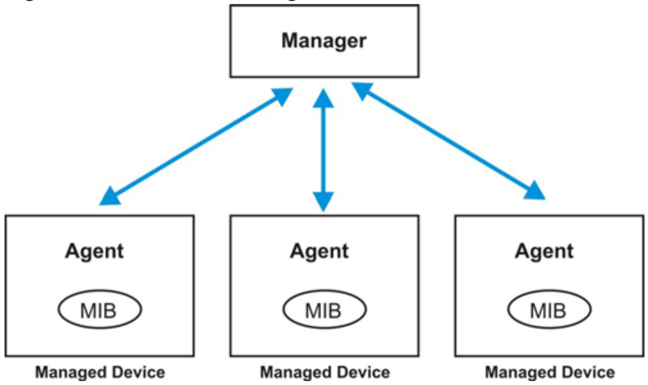
47.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

47.7.1 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 316 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 or 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 or response protocol based on the manager or agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 218 SNMP Commands

LABEL	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.

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.

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

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 219 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.
	zyHwMonitorFANSpeedOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.26.2.6	This trap is sent when the fan speed is recovered from the out of range to normal operating range.
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.
	zyHwMonitorTemperatureOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.26.2.7	This trap is sent when the temperature is recovered from the out of range to 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.
	zyDateTimeTrapTimeServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.82.3.2	This trap is sent when the Switch’s real time clock is up to date.
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.
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.

Table 219 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
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.
	zyPoePowerPortOverloadRecovered	1.3.6.1.4.1.890.1.15.3.59.4.5	This trap is sent when the port is turned on to recover from an overloaded state.
	zyPoePowerPortShortCircuitRecovered	1.3.6.1.4.1.890.1.15.3.59.4.6	This trap is sent when the port is turned on to recover from a short circuit.
	zyPoePowerPortOverSystemBudgetRecovered	1.3.6.1.4.1.890.1.15.3.59.4.7	This trap is sent when the port is turned on to recover from an over system budget.
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 220 SNMP Interface Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
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.

Table 220 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
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.
	zyTransceiverDdmiTemperatureOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.6	This trap is sent when the transceiver temperature is recovered from the out of normal operating range.
	zyTransceiverDdmiTxPowerOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.7	This trap is sent when the transmitted optical power is recovered from the out of normal operating range.
	zyTransceiverDdmiRxPowerOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.8	This trap is sent when the received optical power is recovered from the out of normal operating range.
	zyTransceiverDdmiVoltageOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.9	This trap is sent when the transceiver supply voltage is recovered from the out of normal operating range.
	zyTransceiverDdmiTxBiasOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.10	This trap is sent when the transmitter laser bias current is recovered from the out of 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 221 SNMP 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.
	zyRadiusServerAuthenticationServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.71.2.3	This trap is sent when there is a response message from the previously unreachable RADIUS authentication server.

Table 221 SNMP AAA Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
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.
	zyRadiusServerAccountingServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.71.2.4	This trap is sent when there is a response message from the previously unreachable RADIUS accounting server.

Table 222 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 223 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.
	zyMacForwardingTableFullRecovered	1.3.6.1.4.1.890.1.15.3.48.2.2	This trap is sent when the MAC address switching table has become normal from full.
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.
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.

Table 223 SNMP Switch Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
rip	zyRipExceedMaxDynamicRoute	1.3.6.1.4.1.890.1.15.3.74.2.1	This trap is sent when the maximum allowed number of dynamic routes learned through RIP has been exceeded.
ospf	zyOspfExceedMaxDynamicRoutePath	1.3.6.1.4.1.890.1.15.3.57.3.1	This trap is sent when the maximum allowed number of dynamic routes learned through OSPF has been exceeded.

47.7.2 SSH Overview

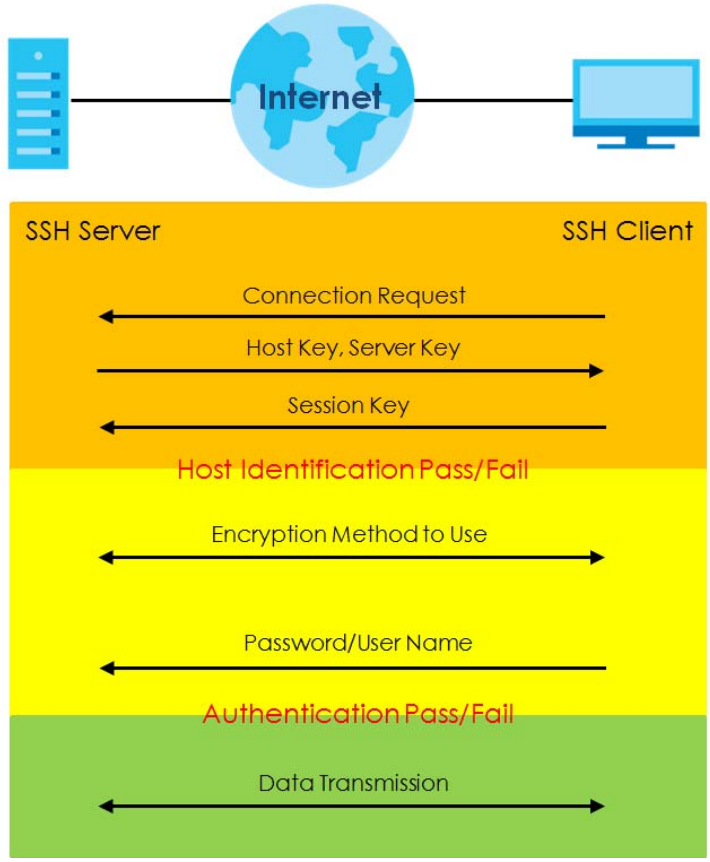
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 317 SSH Communication Example

47.7.2.1 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 318 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.

47.7.2.2 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.

47.7.2.3 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.

47.7.3 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.

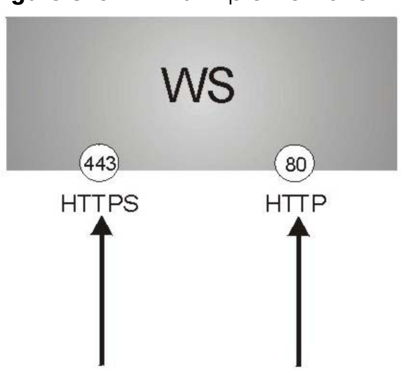
HTTPS on the Switch is used so that you may securely access the Switch using the Web Configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only 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 319 HTTPS Implementation



Note: If you disable HTTP in the Service Access Control screen, then the Switch blocks all HTTP connection attempts.

47.7.3.1 HTTPS Example

If you have not 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.

Internet Explorer Warning Messages

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.

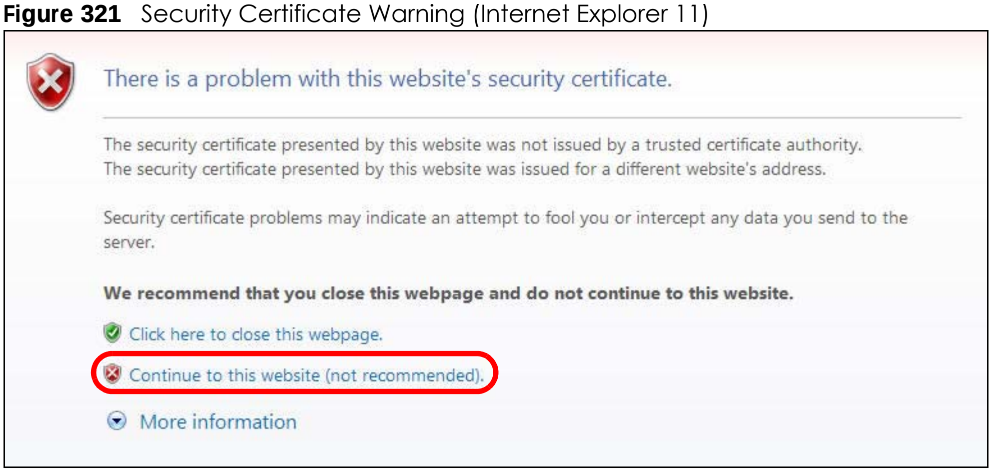
You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the Web Configurator login screen; if you select **No**, then Web Configurator access is blocked.

Figure 320 Security Alert Dialog Box (Internet Explorer 6)

Internet Explorer 7 later version

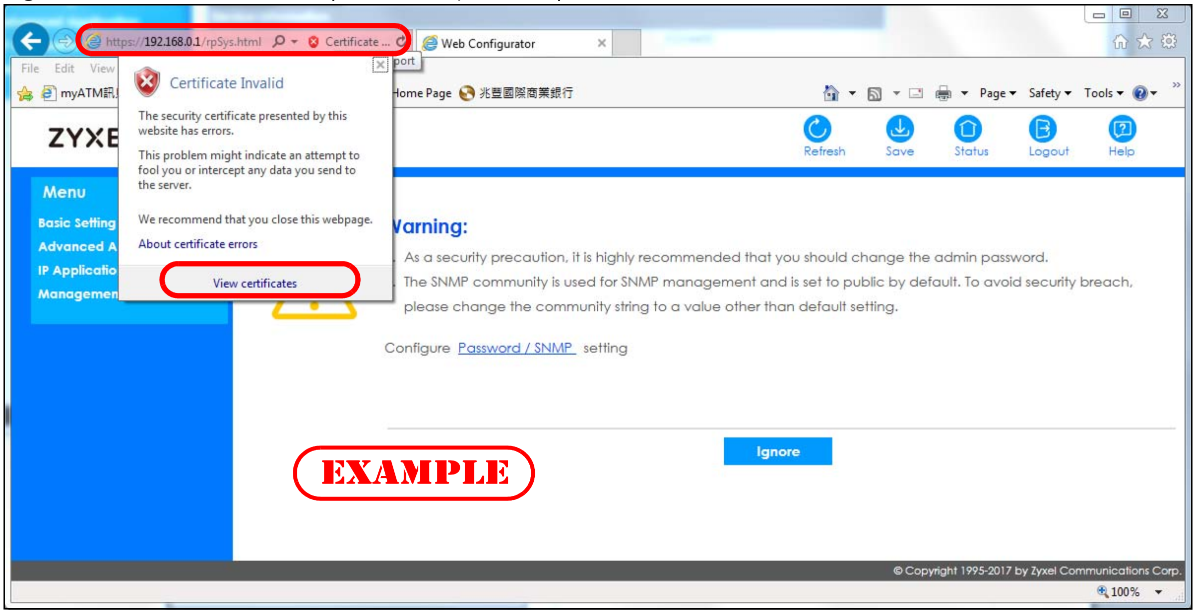
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the Web Configurator login screen.

Figure 321 Security Certificate Warning (Internet Explorer 11)



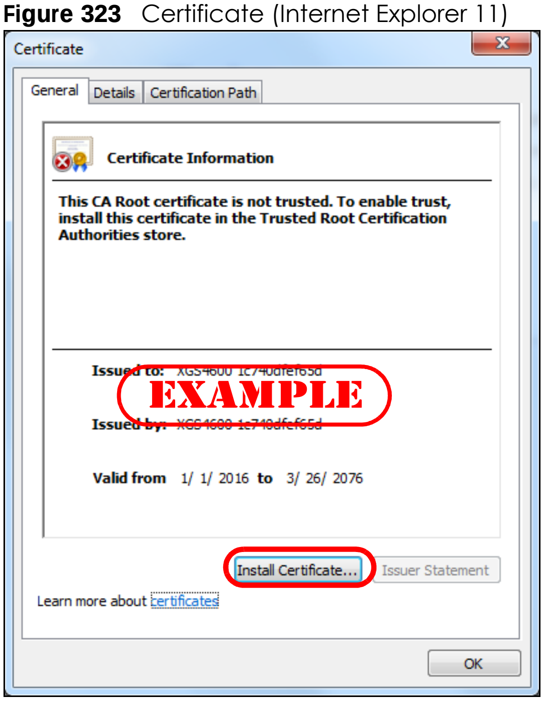
After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 322 Certificate Error (Internet Explorer 11)



Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

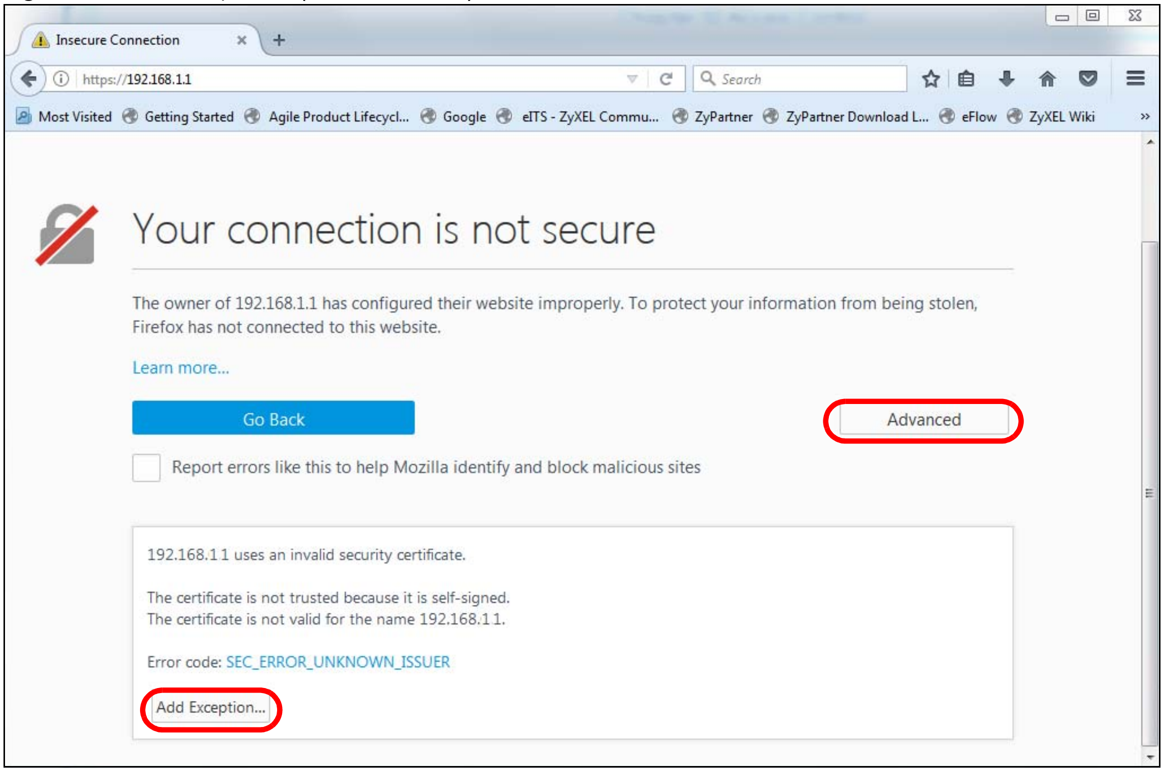
Figure 323 Certificate (Internet Explorer 11)



Mozilla Firefox Warning Messages

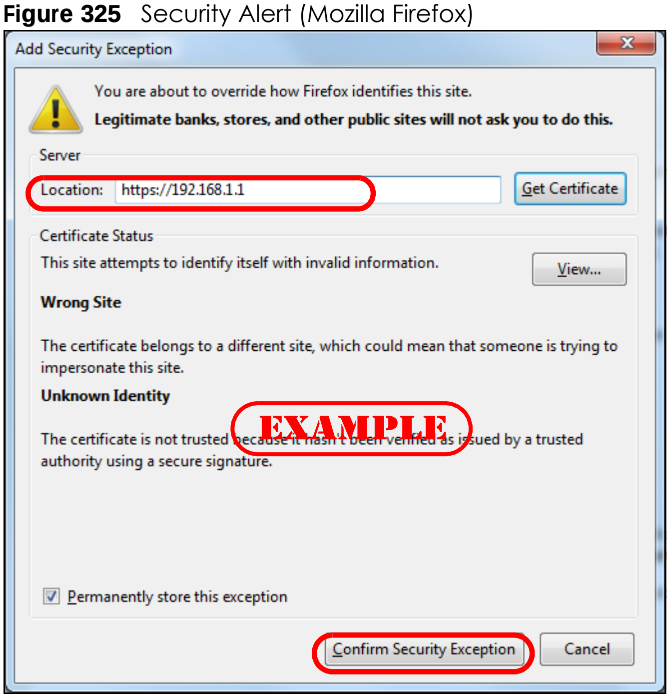
When you attempt to access the Switch HTTPS server, a **Your connection is not secure** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 324 Security Alert (Mozilla Firefox)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the Web Configurator login screen.

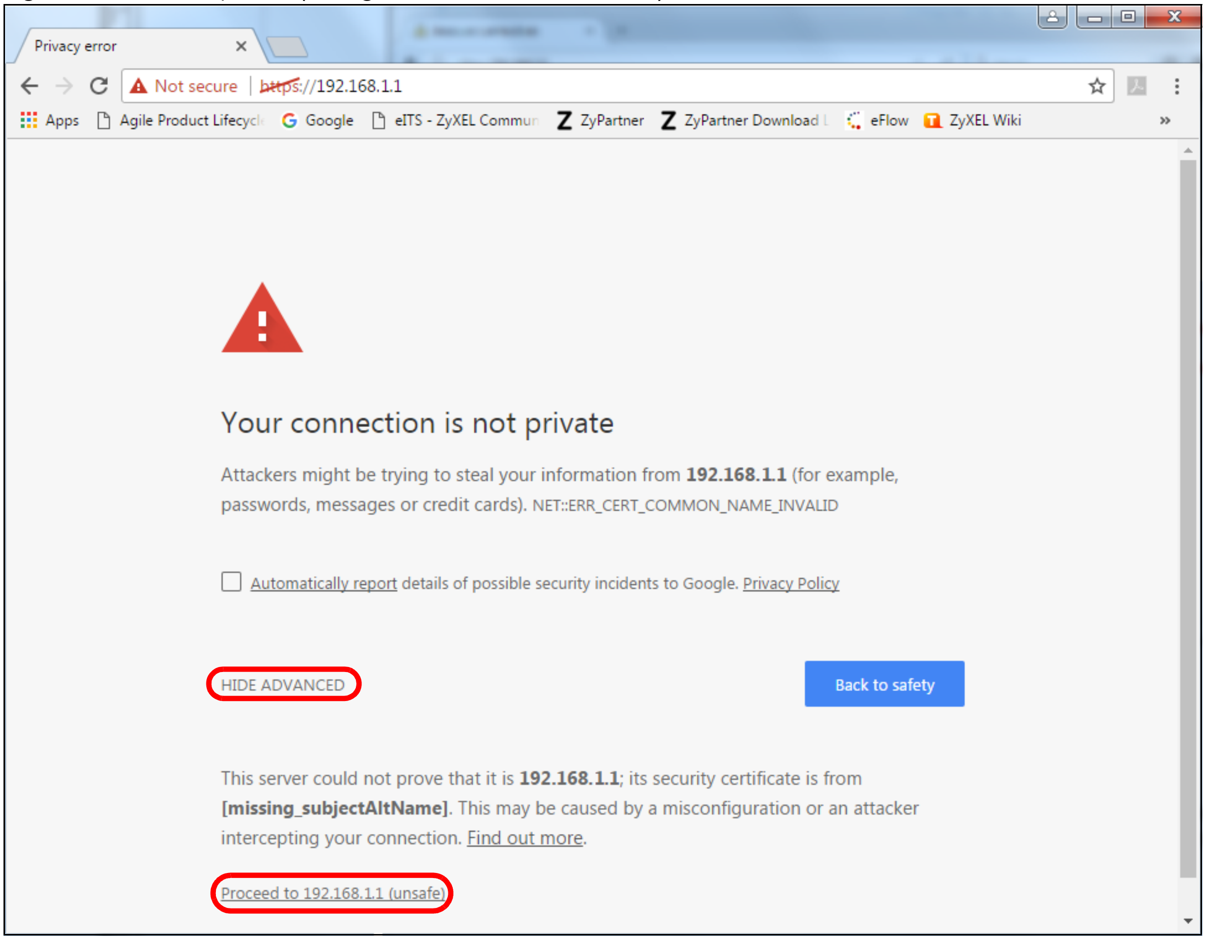
Figure 325 Security Alert (Mozilla Firefox)



47.7.4 Google Chrome Warning Messages

When you attempt to access the Switch HTTPS server, a **Your connection is not private** screen may display. If that is the case, click **Advanced** and then **Proceed to x.x.x.x (unsafe)** to proceed to the Web Configurator login screen.

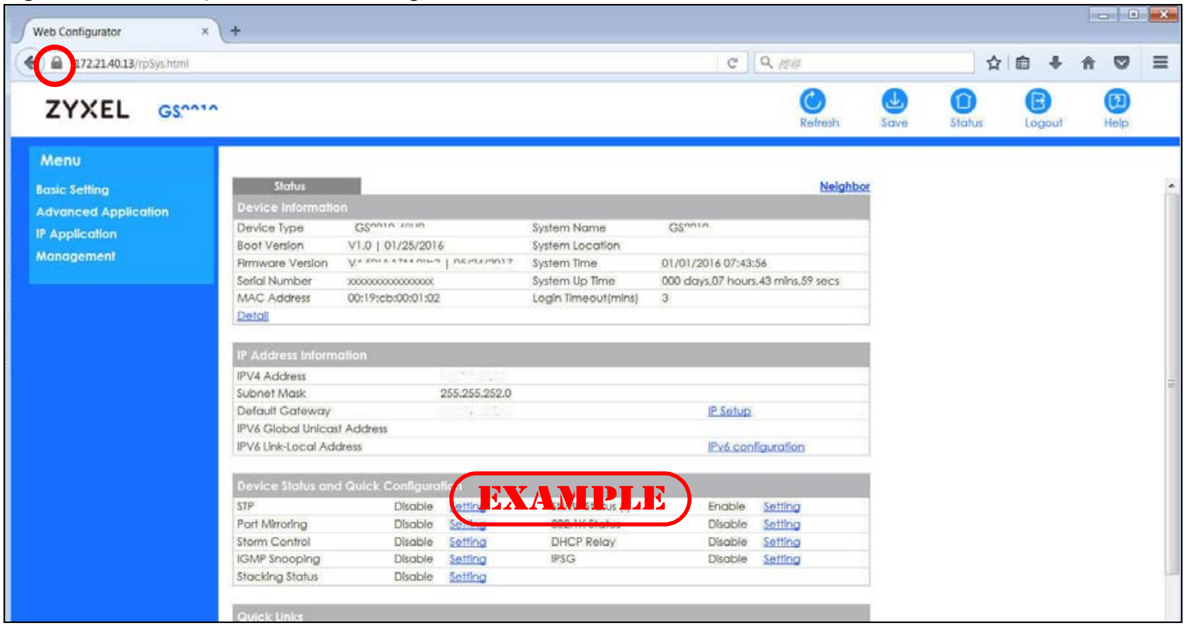
Figure 326 Security Alert (Google Chrome 58.0.3029.110)



47.7.4.1 Main Settings

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 327 Example: Lock Denoting a Secure Connection



CHAPTER 48
Diagnostic

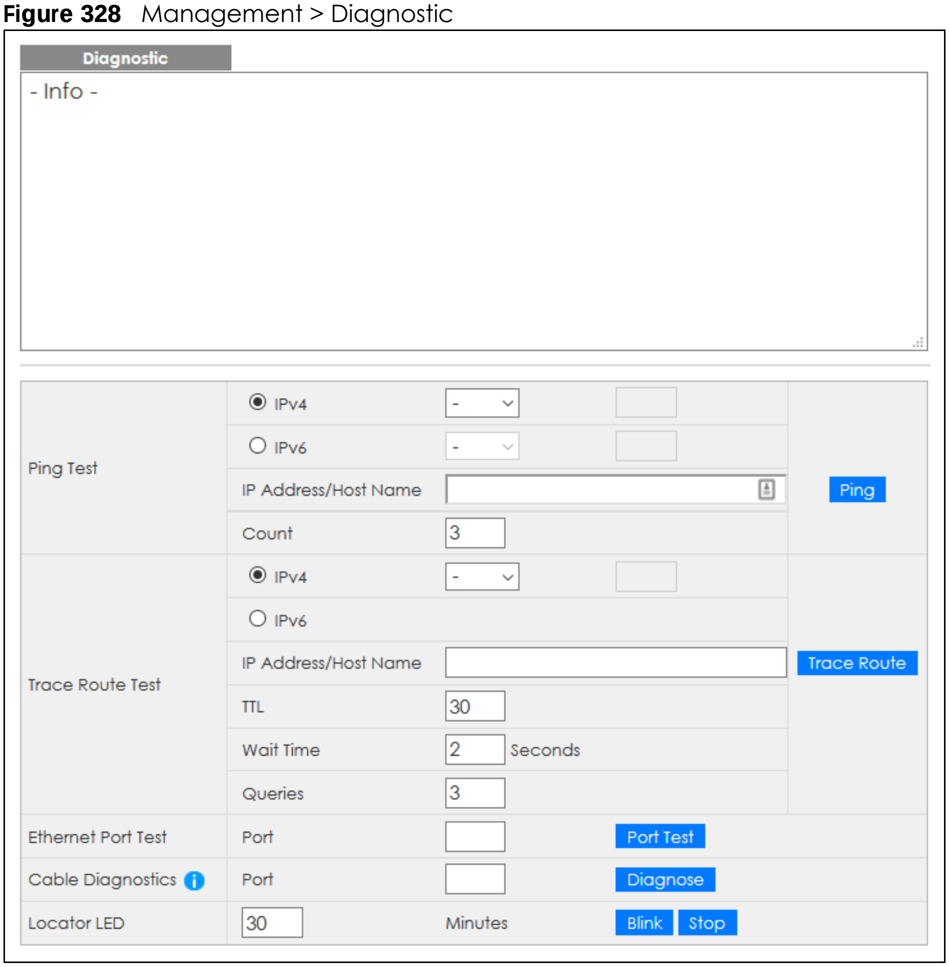
48.1 Overview

This chapter explains the **Diagnostic** screen. You can use this screen to help you identify problems.

48.2 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to ping IP addresses, run a traceroute, perform port tests or show the Switch's location between devices.

Figure 328 Management > Diagnostic



The following table describes the labels in this screen.

Table 224 Management > Diagnostic

LABEL	DESCRIPTION
Ping Test	
IPv4	Select this option if you want to ping an IPv4 address, and select **vlan** to 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.
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.
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.
Count	Enter the number of ICMP Echo Request (ping) messages the Switch continuously sends.
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 **vlan** to specify the ID number of the VLAN on which the Switch traces the path. Otherwise, select **–** to trace the path on any VLAN. Note: The device to which you want to run a traceroute must belong to the VLAN you specify here.
IPv6	Select this option if you want to trace the route packets take to a device with an IPv6 address.
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.
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.
Ethernet Port Test	Enter a port number and click **Port Test** to perform an internal loopback test.
Port	This is the number of the physical Ethernet port on the Switch.
Cable Diagnostics	Enter a port number and click **Diagnose** to perform a physical wire-pair test of the Ethernet connections on the specified ports. The following fields display when you diagnose a port. Note: This feature is limited to within 100 meters only.
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.
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.

Table 224 Management > Diagnostic (continued)

LABEL	DESCRIPTION
Cable length	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	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.
Locator LED	Enter a time interval (in minutes) and click **Blink** to show the actual location of the Switch between several devices in a rack. The default time interval is 30 minutes. Click **Stop** to have the Switch terminate the blinking locater LED.

CHAPTER 49 System Log

49.1 Overview

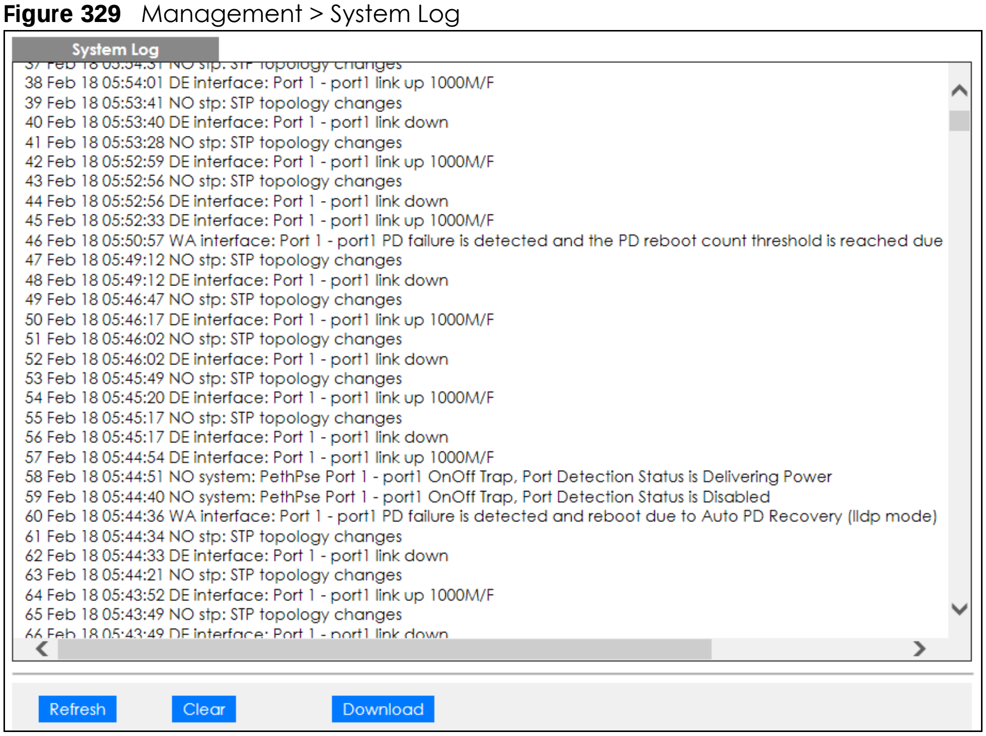
A log message stores the information for viewing.

49.2 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 329 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.

CHAPTER 50
Syslog Setup

50.1 Syslog Overview

This chapter explains the syslog screens.

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 225 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.

50.1.1 What You Can Do

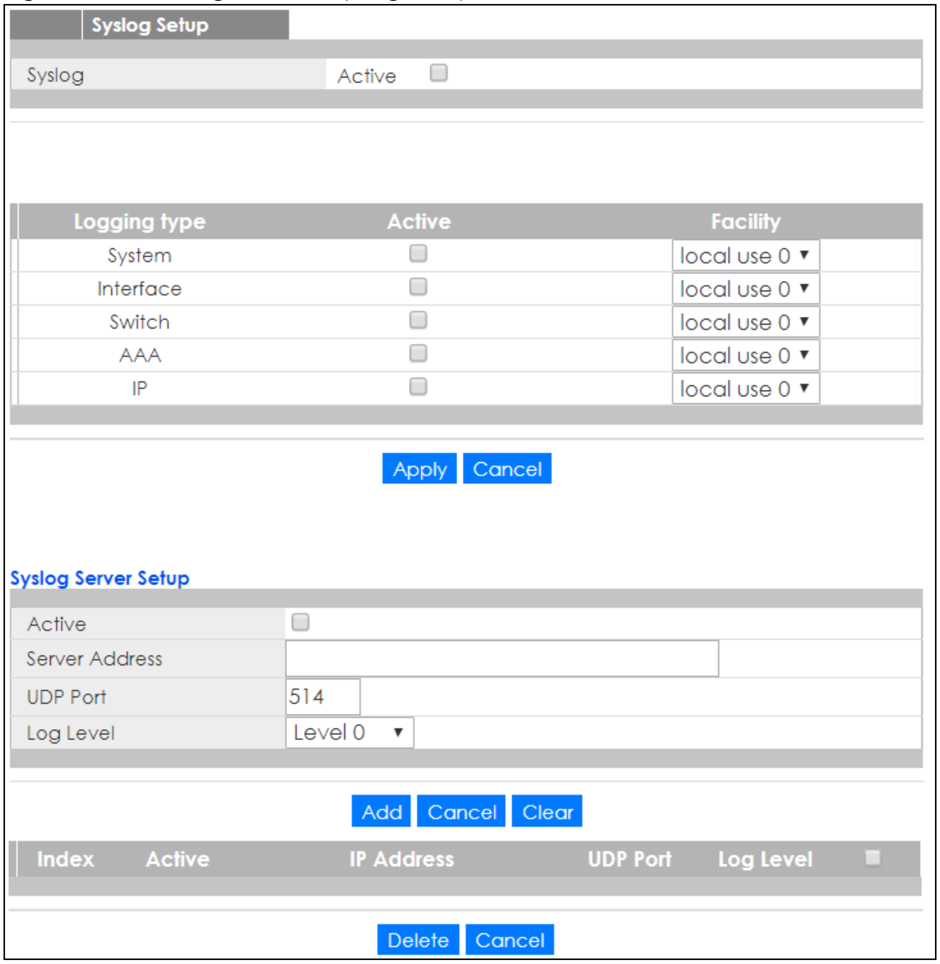
Use the **Syslog Setup** screen (Section 50.2 on page 434) to configure the device's system logging settings and configure a list of external syslog servers.

50.2 Syslog Setup

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.

Click **Management** > **Syslog Setup** in the navigation panel to display this screen.

Figure 330 Management > Syslog Setup



The following table describes the labels in this screen.

Table 226 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 IPv4 or IPv6 address of the syslog server.
UDP Port	The default syslog server port is 514. If your syslog server uses a different port, configure the one it uses here.

Table 226   Management > Syslog Setup (continued)

LABEL	DESCRIPTION
Log Level	Select the severity levels of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **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.
UDP Port	This field displays the port 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 entries.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 51 Cluster Management

51.1 Cluster Management Overview

This chapter introduces cluster management.

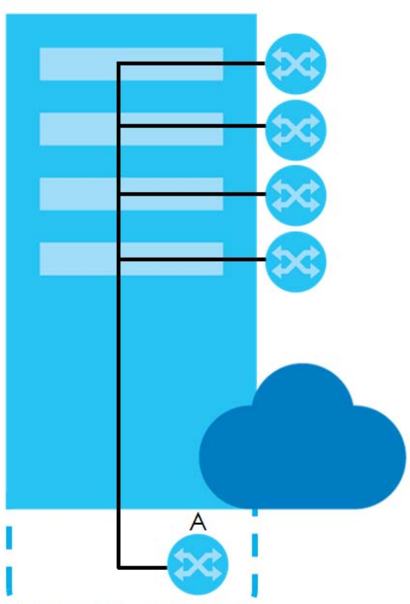
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 227 Zyxel Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with Zyxel cluster management implementation.
Cluster Manager	The Switch through which you manage the cluster member switches.
Cluster Members	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 331 Clustering Application Example



51.1.1 What You Can Do

- Use the **Cluster Management Status** screen (Section 51.2 on page 438) to view the role of the Switch within the cluster and to access a cluster member Switch's Web Configurator.
- Use the **Clustering Management Configuration** screen (Section 51.1 on page 437) to configure clustering management.

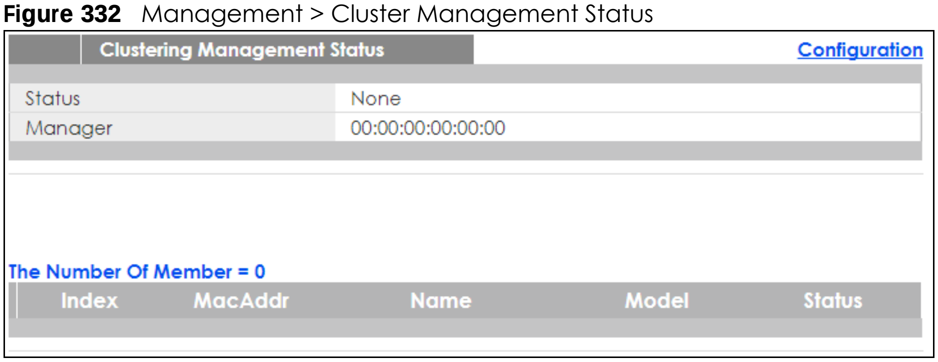
51.2 Cluster Management Status

Use this screen to view the role of the Switch within the cluster and to access a cluster member Switch's Web Configurator.

Click **Management** > **Cluster Management** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 332 Management > Cluster Management Status



The following table describes the labels in this screen.

Table 228 Management > Cluster Management Status

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.
MacAddr	This is the cluster member Switch's hardware MAC address.
Name	This is the cluster member Switch's **System Name**.

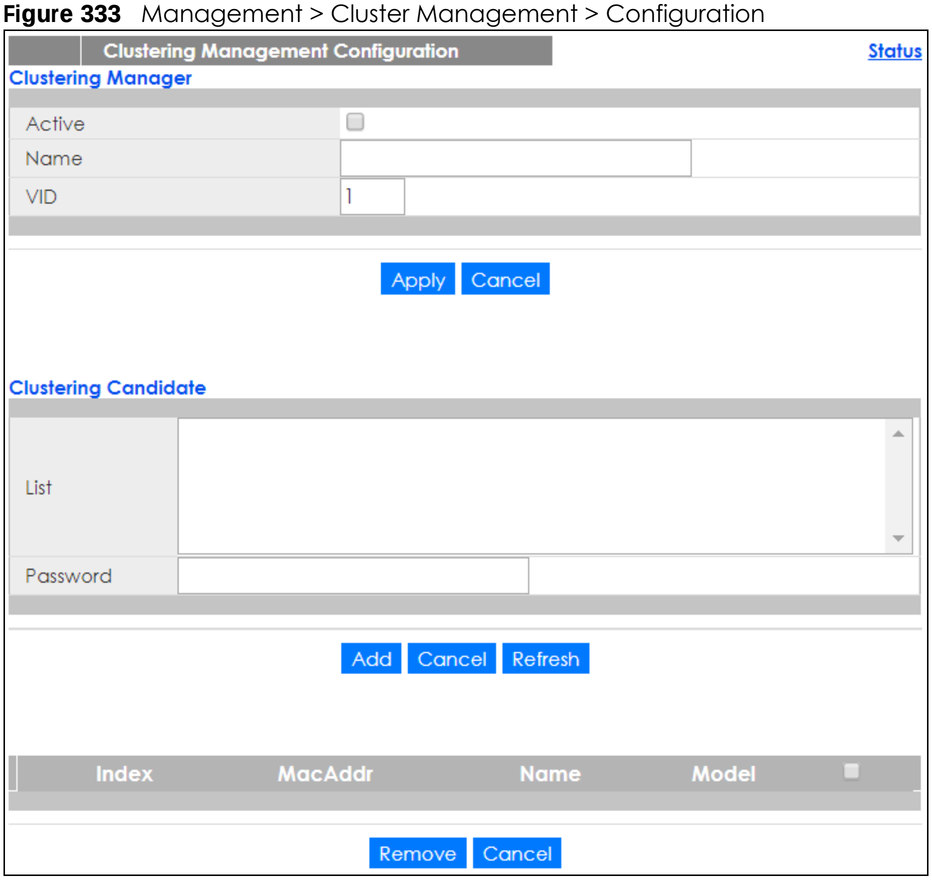
Table 228 Management > Cluster Management Status (continued)

LABEL	DESCRIPTION
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, and so on) **Offline** (the Switch is disconnected – **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

51.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Management** > **Cluster Management** > **Configuration** to display the next screen.

Figure 333 Management > Cluster Management > Configuration



The following table describes the labels in this screen.

Table 229 Management > Cluster Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	The following fields relate to configuring the cluster 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 and a warning icon ( ) 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 switches from the cluster.
Cancel	Click **Cancel** to begin configuring this screen afresh.

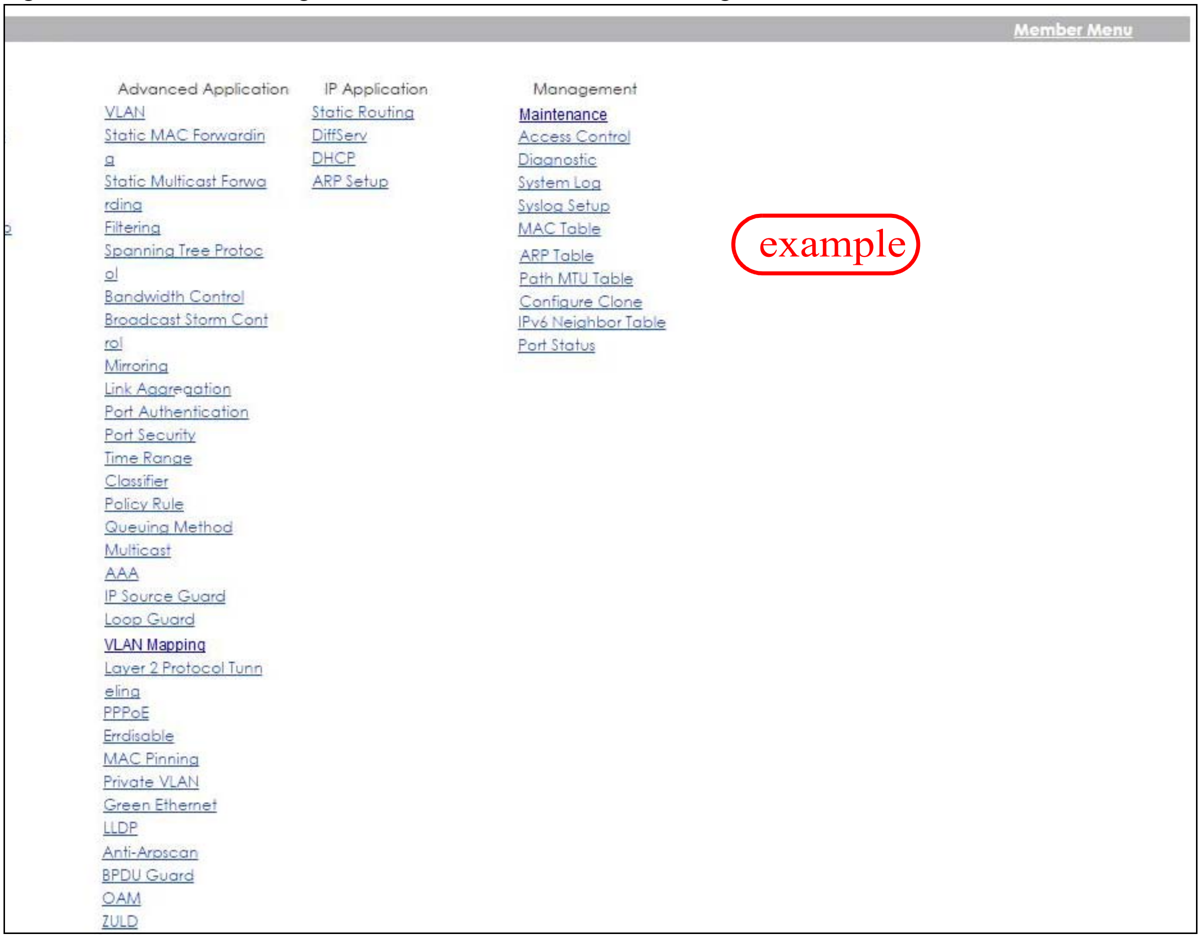
51.4 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

51.4.1 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 would see if you accessed it directly are different.

Figure 334 Cluster Management: Cluster Member Web Configurator Screen



51.4.1.1 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 335 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         3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-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 460ABPI0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-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 230 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.
`460ABPI0.bin`	This is the name of the firmware file you want to upload to the cluster member switch.
`fw-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.

CHAPTER 52
MAC Table

52.1 MAC Table Overview

This chapter introduces the **MAC Table** screen.

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which ports and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

52.1.1 What You Can Do

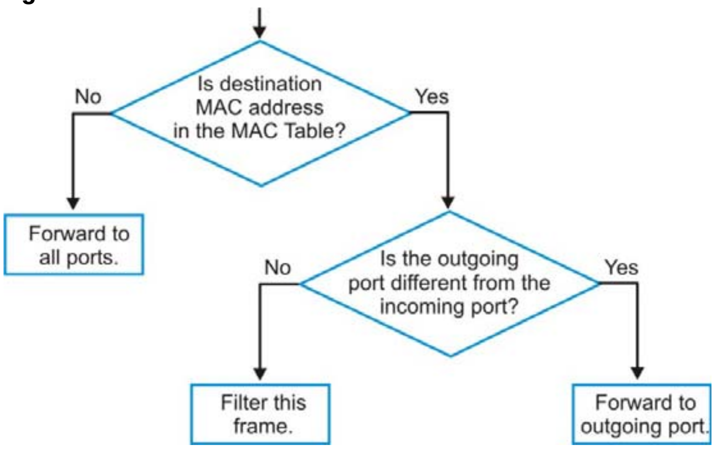
Use the **MAC Table** screen (Section 52.2 on page 444) to check whether the MAC address is dynamic or static.

52.1.2 What You Need to Know

The Switch uses the MAC table to determine how to forward frames. See the following figure.

1. The Switch examines a received frame and learns the port on which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
    - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
    - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion 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 336 MAC Table Flowchart

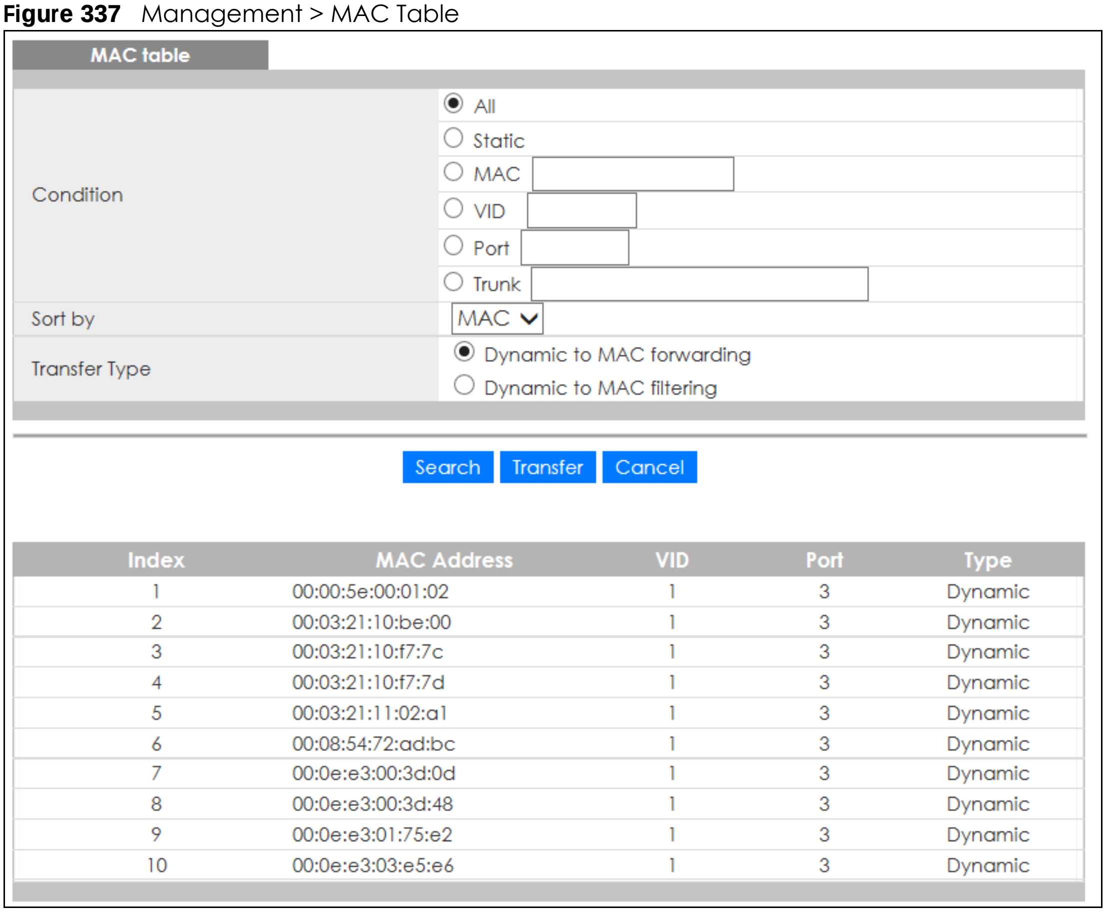


52.2 Viewing the MAC Table

Use this screen to search specific MAC addresses. You can also directly add dynamic MAC addresses into the static MAC forwarding table or MAC filtering table from the MAC table using this screen.

Click **Management** > **MAC Table** in the navigation panel to display the following screen.

Figure 337 Management > MAC Table



Index	MAC Address	VID	Port	Type
1	00:00:5e:00:01:02	1	3	Dynamic
2	00:03:21:10:be:00	1	3	Dynamic
3	00:03:21:10:f7:7c	1	3	Dynamic
4	00:03:21:10:f7:7d	1	3	Dynamic
5	00:03:21:11:02:a1	1	3	Dynamic
6	00:08:54:72:ad:bc	1	3	Dynamic
7	00:0e:e3:00:3d:0d	1	3	Dynamic
8	00:0e:e3:00:3d:48	1	3	Dynamic
9	00:0e:e3:01:75:e2	1	3	Dynamic
10	00:0e:e3:03:e5:e6	1	3	Dynamic

The following table describes the labels in this screen.

Table 231 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select one of the buttons and click **Search** to only display the data which matches the criteria you specified. Select **All** to display any entry in the MAC table of the Switch. Select **Static** to display the MAC entries manually configured on the Switch. Select **MAC** and enter a MAC address in the field provided to display a specified MAC entry. Select **VID** and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN. Select **Port** and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port. Select **Trunk** and type the ID of a trunk group to display all MAC addresses learned from the port(s) in the trunk group.
Sort by	Define how the Switch displays and arranges the data in the summary table below. Select **MAC** to display and arrange the data according to MAC address. Select **VID** to display and arrange the data according to VLAN group. Select **PORT** to display and arrange the data according to port number.
Transfer Type	Select **Dynamic to MAC forwarding** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into static entries. They also display in the **Static MAC Forwarding** screen. Select **Dynamic to MAC filtering** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into MAC filtering entries. These entries will then display only in the **Filtering** screen and the default filtering action is **Discard source**.
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.
Cancel	Click **Cancel** to change the fields back to their last saved values.
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 where the above MAC address is forwarded.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

CHAPTER 53
ARP Table

53.1 Overview

This chapter introduces ARP Table.

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.

53.1.1 What You Can Do

Use the **ARP Table** screen (Section 53.2 on page 446) to view IP-to-MAC address mappings.

53.1.2 What You Need to Know

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.

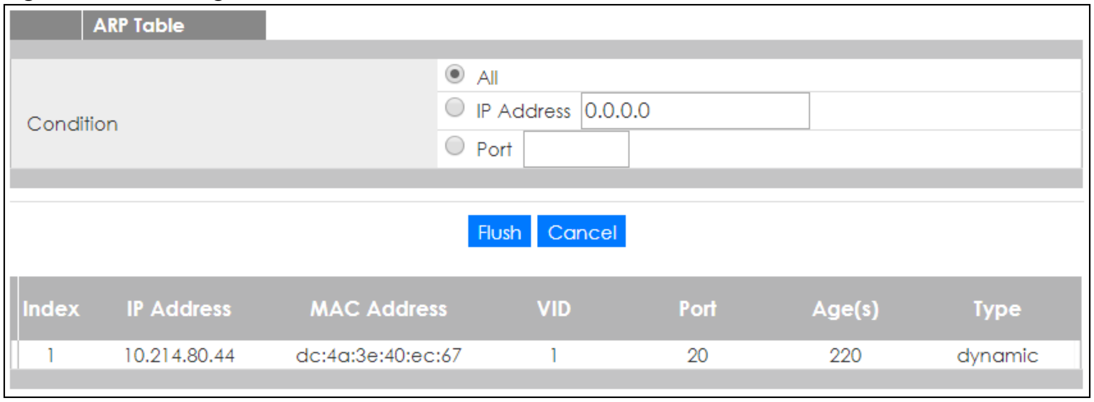
If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target 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.

53.2 Viewing the ARP Table

Use the ARP table to view IP-to-MAC address mappings and remove specific dynamic ARP entries.

Click **Management** > **ARP Table** in the navigation panel to open the following screen.

Figure 338 Management > ARP Table



The following table describes the labels in this screen.

Table 232 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.
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 the IP address is dynamic (learned by the Switch).

CHAPTER 54
Path MTU Table

54.1 Path MTU Overview

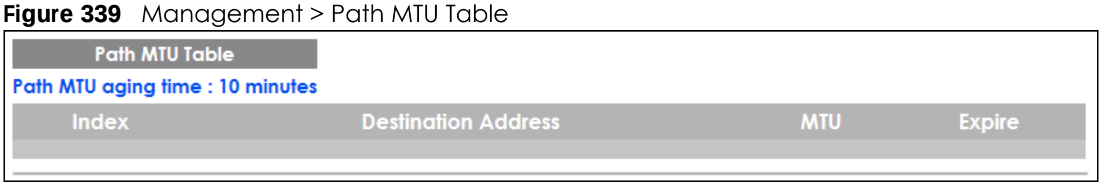
This chapter introduces the IPv6 Path MTU table.

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.

54.2 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 339 Management > Path MTU Table



The following table describes the labels in this screen.

Table 233 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 or 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.

CHAPTER 55
Configure Clone

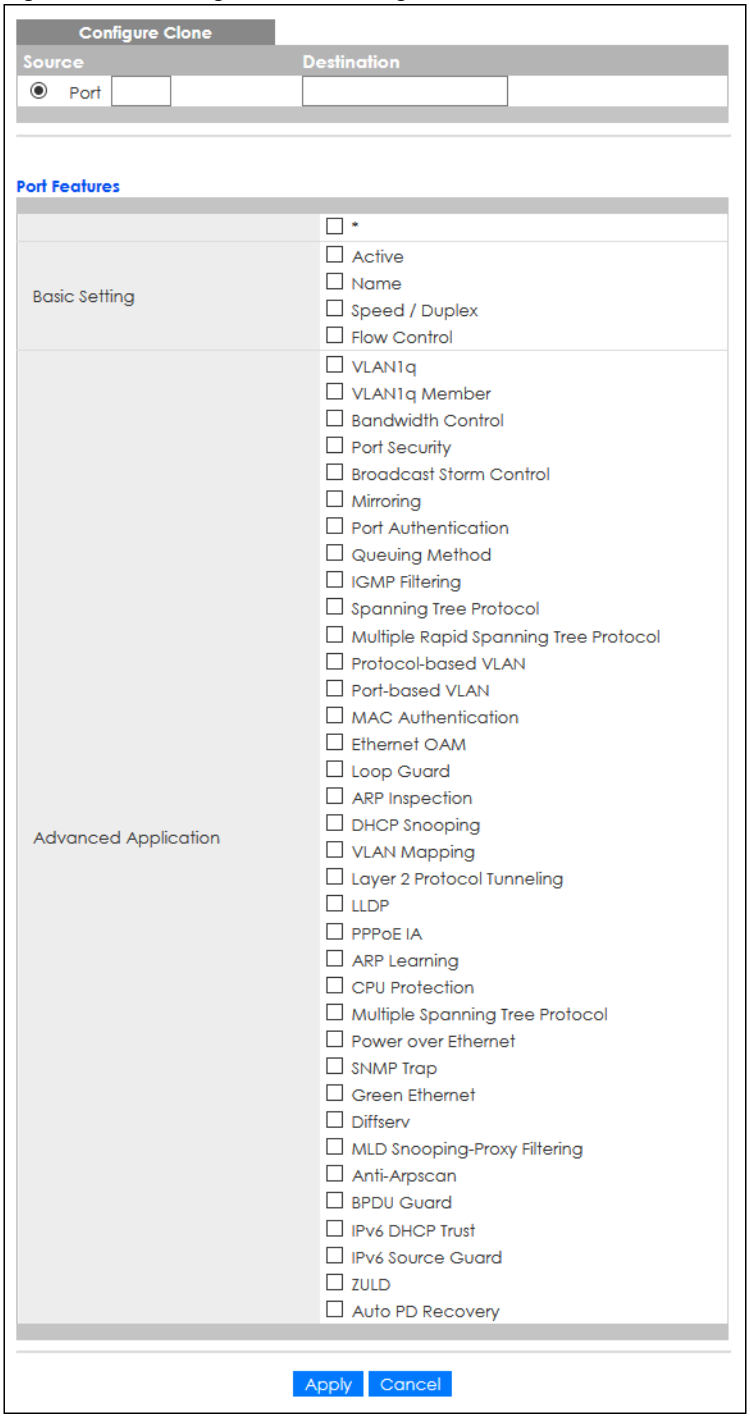
55.1 Overview

This chapter shows you how you can copy the settings of one port onto other ports.

55.2 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 340 Management > Configure Clone



The following table describes the labels in this screen.

Table 234 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port 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 dash. 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.
Source/ Destination	In stacking mode, a port is defined by a slot ID representing the Switch in the stack and a port number. 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 * to apply all settings to the port. Use this first to select the common settings and then remove the settings you do not want copied. Select which port settings (you configured in the **Basic Setting** menus) should be copied to the destination ports.
Advanced Application	Select which port settings (you 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.

CHAPTER 56
IPv6 Neighbor Table

56.1 IPv6 Neighbor Table Overview

This chapter introduces the IPv6 neighbor table.

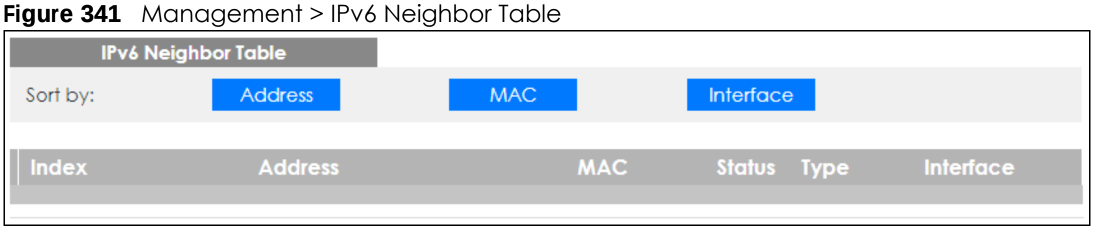
An IPv6 host is required to have a neighbor table. If there is an address to be resolved or verified, the Switch sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor table. You can also manually 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.

56.2 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 341 Management > IPv6 Neighbor Table



The following table describes the labels in this screen.

Table 235 Management > IPv6 Neighbor Table

LABEL	DESCRIPTION
Sort by	Select this to display and arrange the data according to IPv6 address (**Address**), MAC address (**MAC**) or IPv6 interface (**Interface**). The information is then displayed in the summary table below.
Index	This field displays the index number of each entry in the table.
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 configured or the MAC address of the neighboring device.

Table 235 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 cannot 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.
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.

CHAPTER 57
Port Status

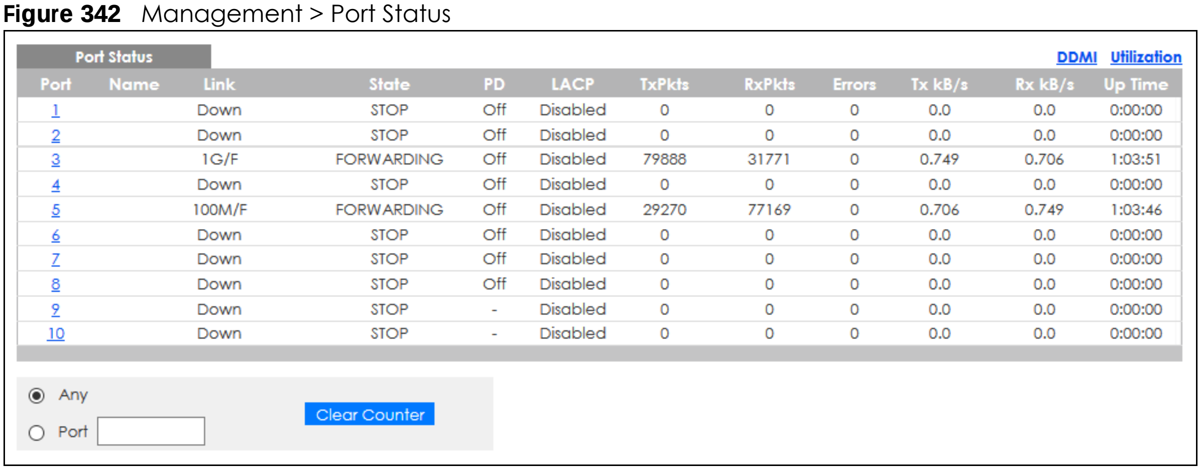
57.1 Overview

This chapter introduces the port status screens.

57.2 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 342 Management > Port Status



Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx kB/s	Rx kB/s	Up Time
1		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
3		1G/F	FORWARDING	Off	Disabled	79888	31771	0	0.749	0.706	1:03:51
4		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
5		100M/F	FORWARDING	Off	Disabled	29270	77169	0	0.706	0.749	1:03:46
6		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00

The following table describes the labels in this screen.

Table 236 Management > Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen.
Name	This is the name you assigned to this port in the **Basic Setting** > **Port Setup** screen.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half). It also shows the cable type (**Copper** or **Fiber**) for the combo ports. 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. If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**. When LACP (Link Aggregation Control Protocol) and STP are in blocking state, it displays **Blocking**.

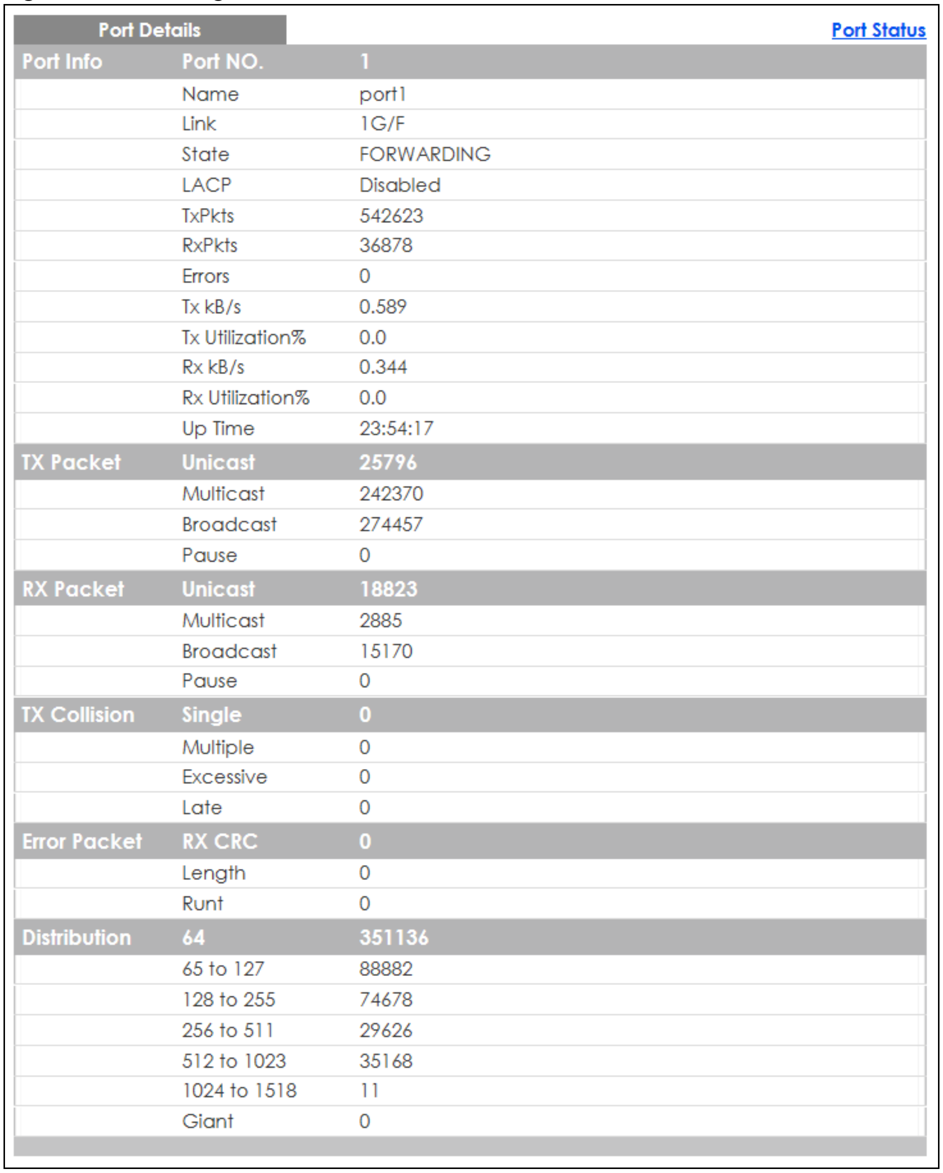
Table 236 Management > Port Status (continued)

LABEL	DESCRIPTION
PD	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 number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Select **Port**, enter 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.

57.2.1 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 343 Management > Port Status > Port Details



Port Details — Port Status

Port Info	Port NO.	1
	Name	port1
	Link	1G/F
	State	FORWARDING
	LACP	Disabled
	TxPkts	542623
	RxPkts	36878
	Errors	0
	Tx kB/s	0.589
	Tx Utilization%	0.0
	Rx kB/s	0.344
	Rx Utilization%	0.0
	Up Time	23:54:17
TX Packet	**Unicast**	**25796**
	Multicast	242370
	Broadcast	274457
	Pause	0
RX Packet	**Unicast**	**18823**
	Multicast	2885
	Broadcast	15170
	Pause	0
TX Collision	**Single**	**0**
	Multiple	0
	Excessive	0
	Late	0
Error Packet	**RX CRC**	**0**
	Length	0
	Runt	0
Distribution	**64**	**351136**
	65 to 127	88882
	128 to 255	74678
	256 to 511	29626
	512 to 1023	35168
	1024 to 1518	11
	Giant	0

The following table describes the labels in this screen.

Table 237 Management > Port Status > Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**) for the combo ports. 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. If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**. When LACP (Link Aggregation Control Protocol), STP, and dot1x are in blocking state, it displays **Blocking**.

Table 237 Management > Port Status > Port Details (continued)

LABEL	DESCRIPTION
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.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx kB/s	This field shows the number of kilobytes per second transmitted on this port.
Tx Utilization%	This field shows the percentage of actual transmitted frames on this port as a percentage of the **Link** speed.
Rx kB/s	This field shows the number of kilobytes per second received on this port.
Rx Utilization%	This field shows the percentage of actual received frames on this port as a percentage of the **Link** speed.
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.
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.
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) errors.
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.

Table 237 Management > Port Status > Port Details (continued)

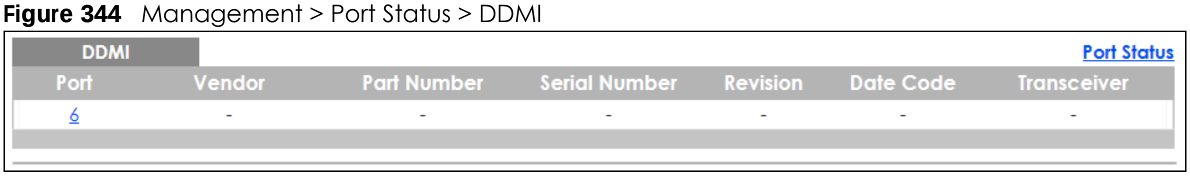
LABEL	DESCRIPTION
128 to 255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256 to 511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512 to 1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024 to 1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	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.

57.2.2 DDMI

The optical SFP transceiver's support for the Digital Diagnostics Monitoring Interface (DDMI) function lets you monitor the transceiver's parameters to perform component monitoring, fault isolation and failure prediction tasks. This allows proactive, preventative network maintenance to help ensure service continuity.

Use this screen to view the DDMI status of the Switch's SFP transceivers. Click **Management** > **Port Status** > **DDMI** to see the following screen. Alternatively, click **Status** from any Web Configurator screen and then the **Port Status** link in the **Quick Links** section of the **Status** screen to display the **Port Status** screen and then click the **DDMI** link tab.

Figure 344 Management > Port Status > DDMI



The following table describes the labels in this screen.

Table 238 Management > Port Status > DDMI

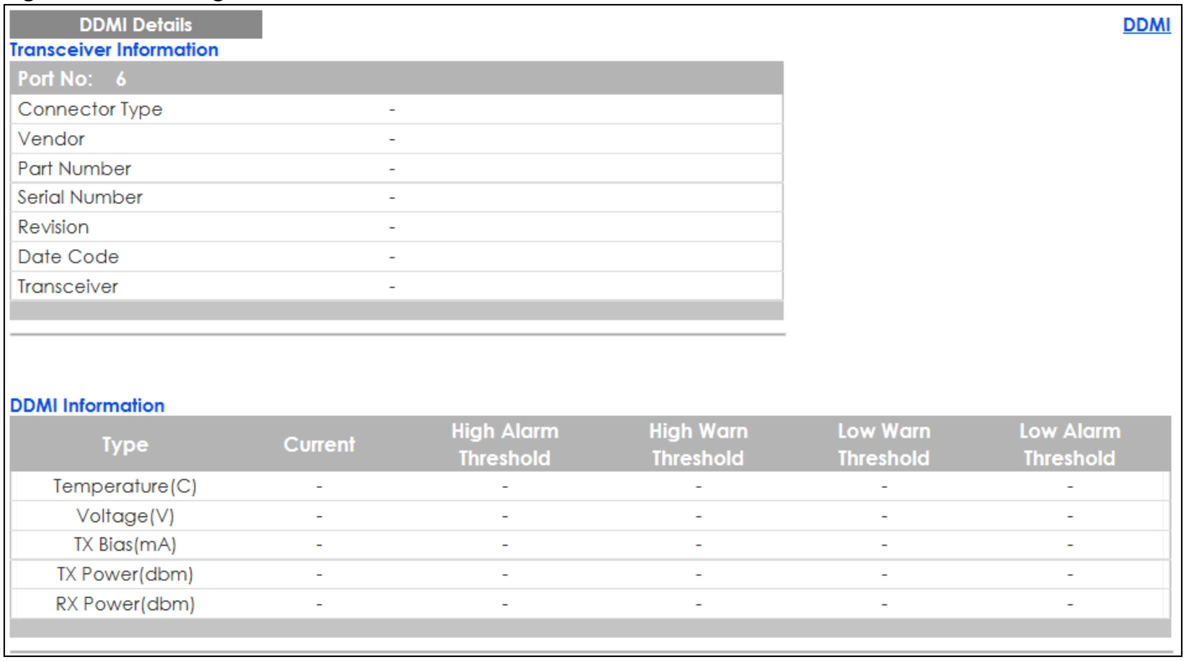
LABEL	DESCRIPTION
Port	This identifies the SFP port.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays whether the connection to the optical network is up or down.

57.2.3 DDMI Details

Use this screen to view the real-time SFP (Small Form Factor Pluggable) transceiver information and operating parameters on the SFP port. The parameters include, for example, transmitting and receiving power, and module temperature.

Click a number in the **Port** column in the **DDMI** screen to view current transceivers' status.

Figure 345 Management > Port Status > DDMI > DDMI Details



The following table describes the labels in this screen.

Table 239 Management > Port Status > DDMI > DDMI Details

LABEL	DESCRIPTION
Transceiver Information	
Port No	This identifies the SFP port.
Connector Type	This displays the connector type of the optical transceiver.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays details about the type of transceiver installed in the SFP slot.
Calibration	This field is available only when an SFP transceiver is inserted into the SFP slot. **Internal** displays if the measurement values are calibrated by the transceiver. **External** displays if the measurement values are raw data which the Switch calibrates.
DDMI Information	
Type	This displays the DDMI parameter.
Temperature (C/F)	This displays the temperature inside the SFP transceiver in degrees Celsius or Fahrenheit.
Voltage (V)	This displays the level of voltage being supplied to the SFP transceiver.
TX Bias (mA)	This displays the milliamps (mA) being supplied to the SFP transceiver's Laser Diode Transmitter.
TX Power (dbm)	This displays the amount of power the SFP transceiver is transmitting.
RX Power (dbm)	This displays the amount of power the SFP transceiver is receiving from the fiber cable.

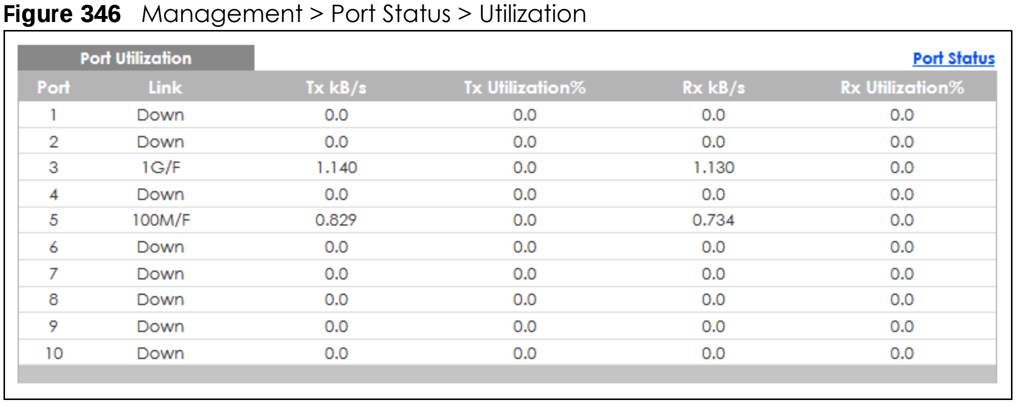
Table 239 Management > Port Status > DDMI > DDMI Details (continued)

LABEL	DESCRIPTION
Current	This displays the current status for each monitored DDMI parameter.
High Alarm Threshold	This displays the high value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the Switch if the monitored DDMI parameter reaches this value.
High Warn Threshold	This displays the high value warning threshold for each monitored DDMI parameter. A warning signal is reported to the Switch if the monitored DDMI parameter reaches this value.
Low Warn Threshold	This displays the low value warning threshold for each monitored DDMI parameter. A warning signal is reported to the Switch if the monitored DDMI parameter reaches this value.
Low Alarm Threshold	This displays the low value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the Switch if the monitored DDMI parameter reaches this value.

57.2.4 Port Utilization

This screen displays the percentage of actual transmitted or received frames on a port as a percentage of the **Link** speed. To view port utilization, click **Management** > **Port Status** > **Port Utilization** to see the following screen. Alternatively, click **Status** from any Web Configurator screen and then the **Port Status** link in the **Quick Links** section of the **Status** screen to display the **Port Status** screen and then click the **Utilization** link tab.

Figure 346 Management > Port Status > Utilization



Port Utilization | Port Status

Port	Link	Tx kB/s	Tx Utilization%	Rx kB/s	Rx Utilization%
1	Down	0.0	0.0	0.0	0.0
2	Down	0.0	0.0	0.0	0.0
3	1G/F	1.140	0.0	1.130	0.0
4	Down	0.0	0.0	0.0	0.0
5	100M/F	0.829	0.0	0.734	0.0
6	Down	0.0	0.0	0.0	0.0
7	Down	0.0	0.0	0.0	0.0
8	Down	0.0	0.0	0.0	0.0
9	Down	0.0	0.0	0.0	0.0
10	Down	0.0	0.0	0.0	0.0

The following table describes the labels in this screen.

Table 240 Management > Port Status > Utilization

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex). It also shows the cable type (**Copper** or **Fiber**) for the combo ports. This field displays **Down** if the port is not connected to any device.
Tx kB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Tx Utilization%	This field shows the percentage of actual transmitted frames on this port as a percentage of the Link speed.
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Rx Utilization%	This field shows the percentage of actual received frames on this port as a percentage of the **Link** speed.

CHAPTER 58
Networked AV Mode

58.1 Overview

Aside from the Web Configurator in Standard mode that has a complete set of configuration for network installation, you can switch to Networked AV mode. Networked AV mode contains just the necessary configurations for setting up and managing audio-video traffic on your network.

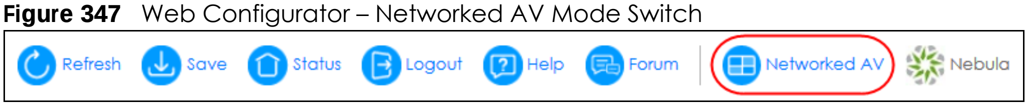
AV over IP is the transmission of audio-video data over an IP network.

Use a browser that supports HTML5, such Microsoft Edge, Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended screen resolution is 1024 by 768 pixels.

The following sections introduces the configuration and functions of the Web Configurator In Networked AV mode.

Click **Networked AV** at the top right corner of the Web Configurator to switch between the Web Configurator's **Standard** or **Networked AV** mode.

Figure 347 Web Configurator – Networked AV Mode Switch

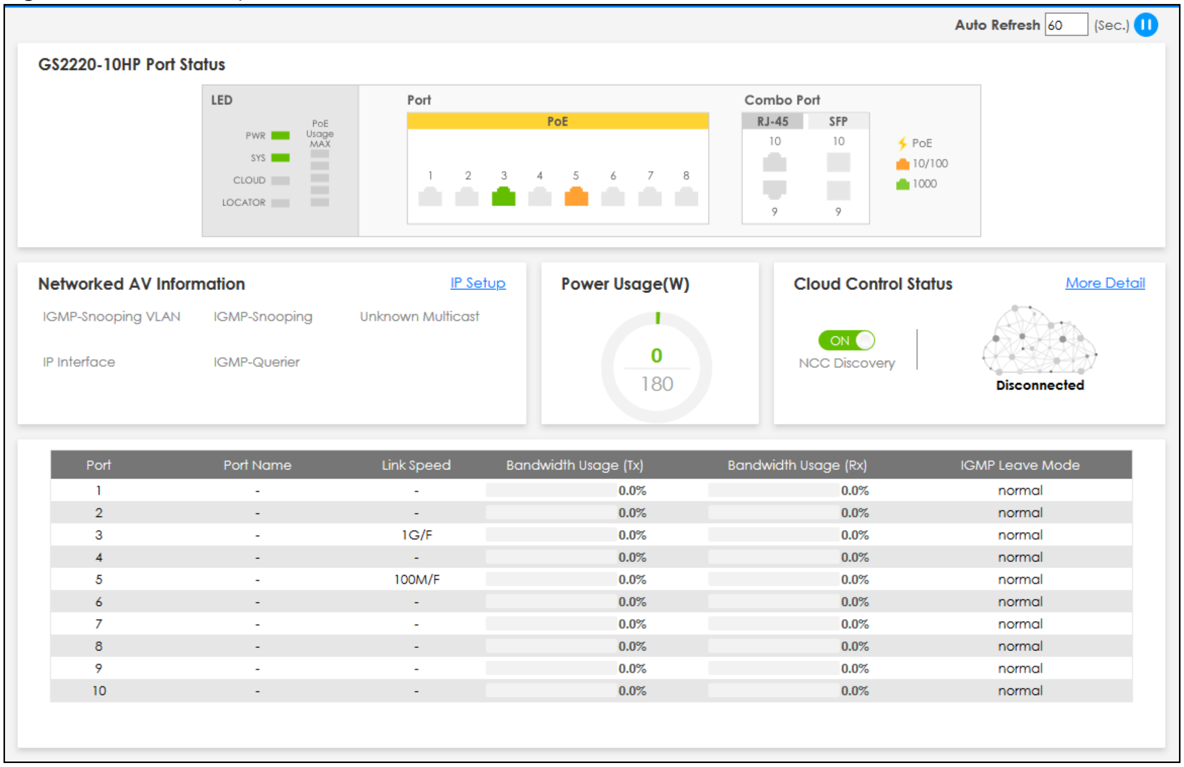


58.2 Summary

Use the **Summary** screen to see the Switch's front panel port status, connected ports information, networked AV information, used power for PoE devices, Nebula Cloud Control status, and a link to go to the **IP Setup** screen (Section 62.1 on page 499).

The **Summary** screen displays when you log into the Switch in Networked AV mode.

Figure 348 Summary



The following table describes the labels in this screen.

Table 241 Summary

LABEL	DESCRIPTION
Auto Refresh	Enter the number of seconds when the **Summary** screen details will be updated. Click the Pause or Play icon to stop or resume the screen update, or to update the automatic refresh interval.
Port Status	This chart displays the status of the Switch's front panel ports with connection (**LED**, **Port**, and **Combo Port**).
Networked AV Information	
IP Setup	This link takes you to a screen where you can configure the IP address and subnet mask (necessary for Switch management) and set up to 64 IP routing domains.
IGMP-Snooping VLAN	This displays the ID number of the VLAN group upon which the Switch is to perform IGMP snooping.
IGMP Snooping	This displays **Active** when IGMP snooping is enabled to forward group multicast traffic only to ports that are members of that group. Otherwise, it is **Inactive**.
Unknown Multicast	This displays the action to perform when the Switch receives an unknown multicast frame. It displays **Drop** when the frames are discarded. It displays **Flooding** when the frames are sent to all ports. It displays **Drop on VLAN** when the frames are discarded on the specified VLANs.
IP Interface	This displays the IP address of the Switch for it to be managed over the network.
IGMP-Querier	This displays **Active** when the Switch is allowed to send IGMP General Query messages to the VLANs with the multicast hosts attached. Otherwise, it is **Inactive**.

Table 241 Summary (continued)

LABEL	DESCRIPTION
Power Usage(W)	This chart displays the used PoE Watts over the total number of Watts provided on this Switch.
Cloud Control Status	This displays the registration and connection status between the Switch and the NCC (Nebula Control Center). Click **More Detail** to go to **System** > **Cloud Management** screen.
Port	This displays the port of this Switch.
Port Name	This displays the port description of this Switch.
Link Speed	This displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half). This field displays **Down** if the port is not connected to any device.
Bandwidth Usage (Tx) Bandwidth Usage (Rx)	These display the percentage of bandwidth usage on this port as a percentage of the **Link Speed**.
IGMP Leave Mode	This displays **immediate** when the Switch receives IGMP leave packets, the Switch will close the multicast stream immediately without any further action. This displays **fast** when the Switch will further generate a group specific query packet to all the receivers. This could prevent the traffic being cut if some receivers still want to receive the multicast stream. This displays **normal** 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 for this port.

CHAPTER 59
System

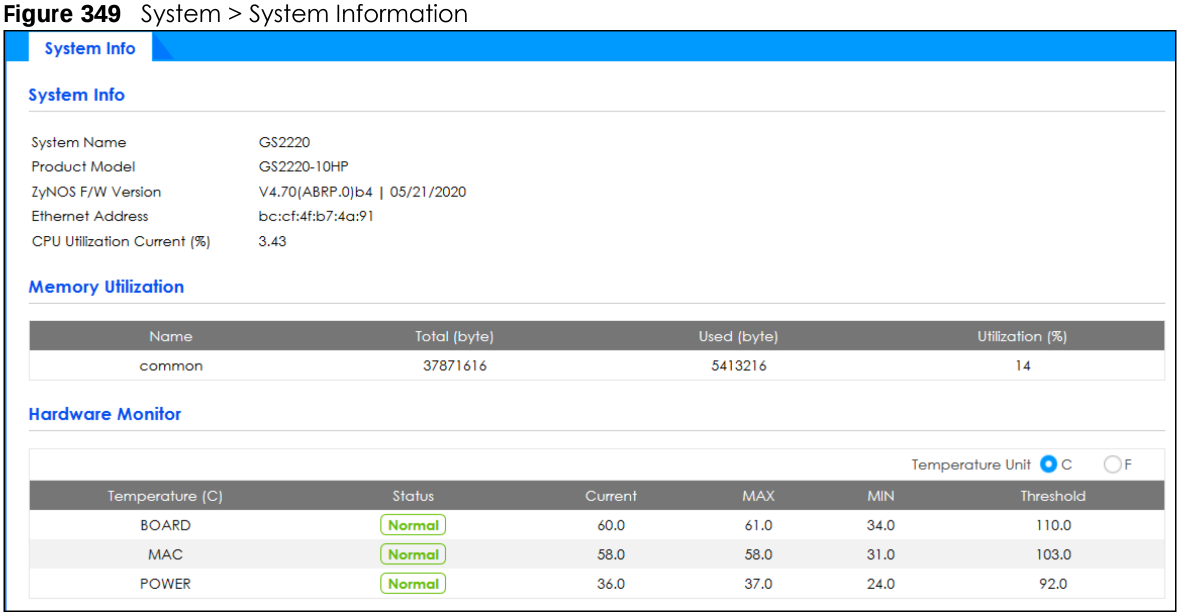
59.1 What You Can Do

- Use the **System Information** screen (Section 59.2 on page 464) to check the firmware version number and monitor the Switch temperature.
- Use the **General Setup** screen (Section 59.3 on page 465) to configure general settings such as the system name and time.
- Use the **Cloud Management** screen (Section 59.4 on page 467) to display links to **Nebula Control Center Discovery** and **Nebula Switch Registration** screens.

59.2 System Information

In the navigation panel, click **System** > **System Information** to display the screen as shown. Use this screen to view general system information. You can check the firmware version number and monitor the Switch temperature.

Figure 349 System > System Information



The following table describes the labels in this screen.

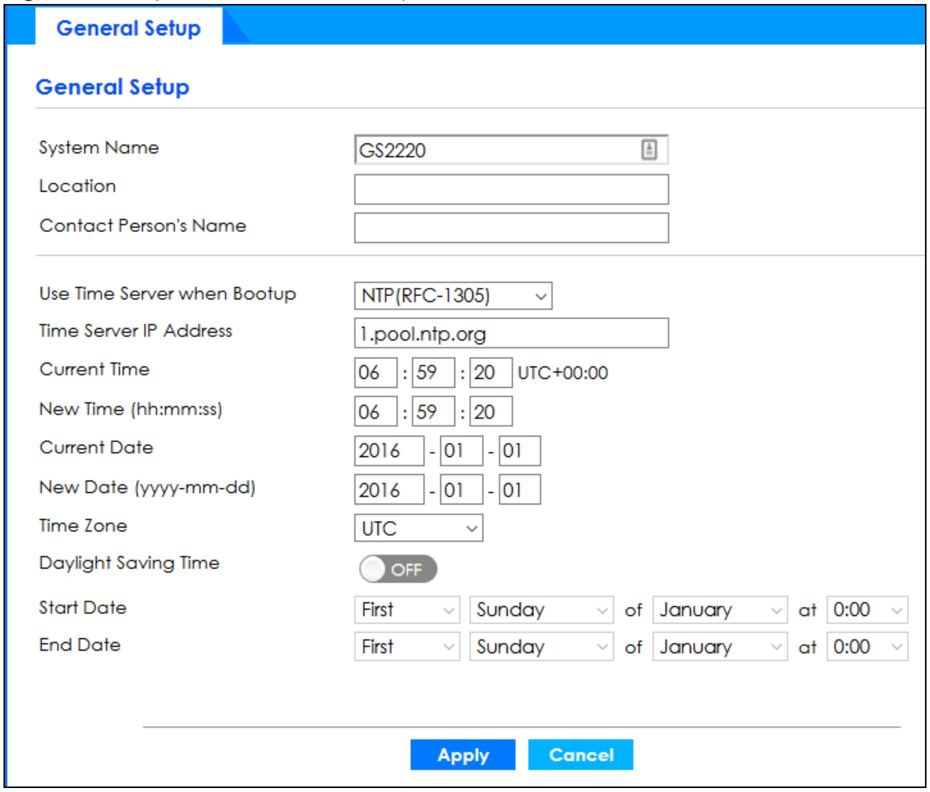
Table 242 System > System Info

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 Current (%)	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 (byte)	This field displays the total number of bytes in this memory pool.
Used (byte)	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	
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 (C)	**BOARD**/**MAC**/**POWER** refers to the location of the temperature sensor on the Switch printed circuit board.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
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.

59.3 General Setup

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

Figure 350 System > General Setup



The following table describes the labels in this screen.

Table 243 System > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Enter the time service protocol that your time server 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 0:0:0.
Time Server IP Address	Enter the IP address or domain name of your timeserver. The Switch searches for the timeserver for up to 60 seconds.
Current Time	This field displays the time you open this menu (or refresh the menu).

Table 243 System > General Setup (continued)

LABEL	DESCRIPTION
New Time (hh:mm: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. Set the switch to **ON** 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 first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **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).
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.

59.4 Cloud Management

The Switch supports NebulaFlex which can set the Switch to operate in either standalone or Nebula cloud management mode. When the Switch is in standalone mode, it can be configured and managed by the Web Configurator. When the Switch is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control Center (NCC).

The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula APs, Ethernet switches and security gateways.

Note: NebulaFlex for hybrid mode and NCC registration are NOT supported at the time of writing and reserved for future use.

The Switch is managed and provisioned automatically by the NCC (Nebula Control Center) when:

- The Switch is connected to the Internet.
- The **Nebula Control Center Discovery** feature is enabled.
- The Switch has been registered in the NCC.

The **Cloud Management** screen displays links to **Nebula Switch Registration** which has a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC.

Click **System** > **Cloud Management** in the navigation panel to display this screen.

Figure 351 System > Cloud Management

Select **On** to turn on NCC discovery on the Switch. If the Switch has Internet access and has been registered in the NCC, it will go into cloud management mode.

In cloud management mode, then NCC will first check if the firmware on the Switch needs to be upgraded. If it does, the Switch will upgrade the firmware immediately. If the firmware does not need to be upgraded, but there is newer firmware available for the Switch, then it will be upgraded according to the firmware upgrade schedule for the Switch on the NCC. Below is the process for upgrading firmware:

1. Download firmware via the NCC.
2. Upgrade the firmware and reboot.

Note: While the Switch is rebooting, do NOT turn off the power.

Disable **On** to turn off NCC discovery on the Switch. The Switch will NOT discover the NCC and remain in standalone mode.

This screen has a QR code containing the Switch's serial number and MAC address for handy NCC registration of the Switch using the Nebula Mobile app. First, download the app from the Google Play store for Android devices or the App Store for iOS devices and create an organization and site.

CHAPTER 60 Port

60.1 What You Can Do

- Use the **PoE Status** screen (Section 60.2 on page 469) to view the current amount of power that PDs are receiving from the Switch.
- Use the **PoE Setup** screen (Section 60.3 on page 471) to set the PoE power management mode, priority levels, power-up mode and the maximum amount of power for the connected PDs.
- Use the **Port Setup** screen (Section 60.4 on page 473) to configure Switch port settings.

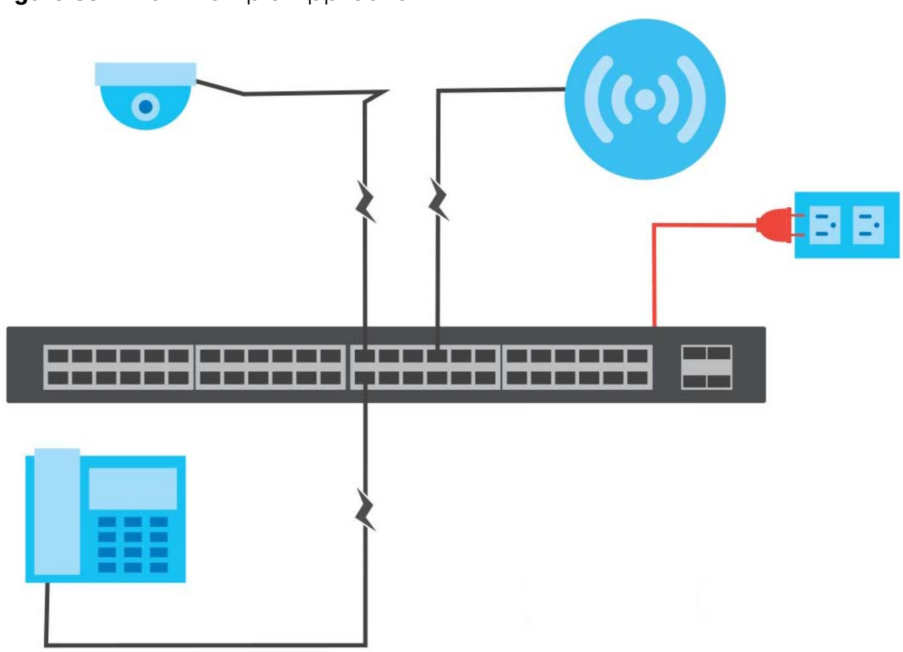
60.2 PoE Status

A powered device (PD) is a device such as an access point or a switch, that supports PoE (Power over Ethernet) so that it can receive power from another device through an Ethernet port.

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

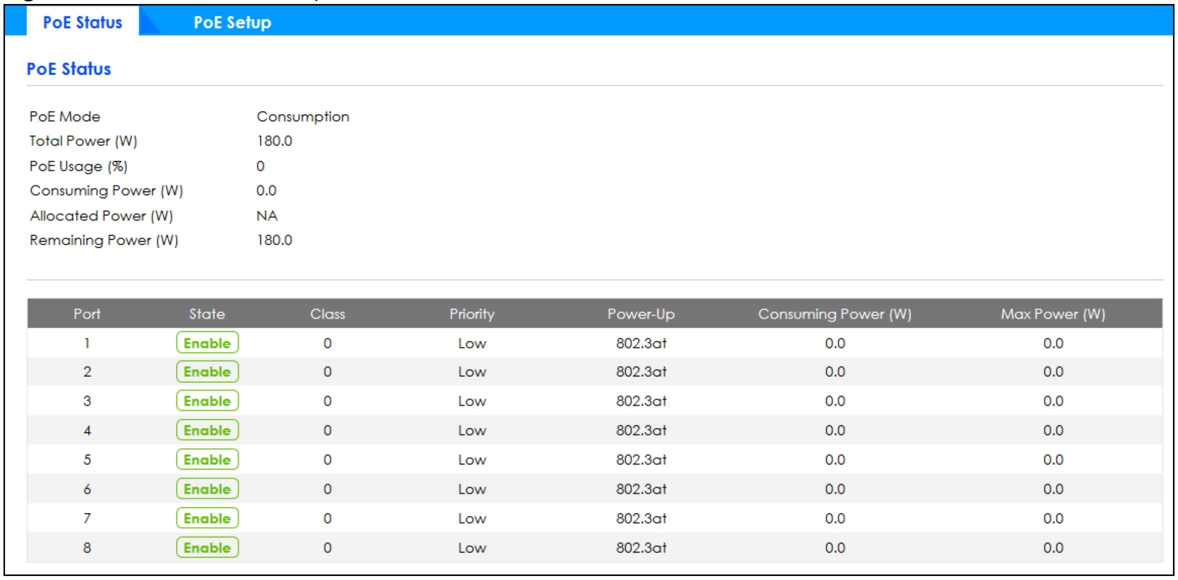
Note: The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

Figure 352 PoE Example Application



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

Figure 353 Port > PoE Setup > PoE Status



The following table describes the labels in this screen.

Table 244 Port > PoE Setup > PoE Status

LABEL	DESCRIPTION
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.
PoE Usage (%)	This field displays the amount of power currently being supplied to connected PoE devices (PDs) as a percentage of the total PoE power the Switch can supply. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in **Port** > **PoE Setup** > **PoE Setup**.
Consuming Power (W)	This field displays the 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 (in classification mode) has reserved for PoE after negotiating with the connected PoE devices. It shows **NA** when the Switch is in consumption mode. **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	This is the port index number.
State	This field shows which ports can receive power from the Switch. You can set this in Section 60.3 on page 471. • **Disable** – The PD connected to this port cannot get power supply. • **Enable** – The PD connected to this port can receive power.

Table 244   Port > PoE Setup > PoE Status (continued)

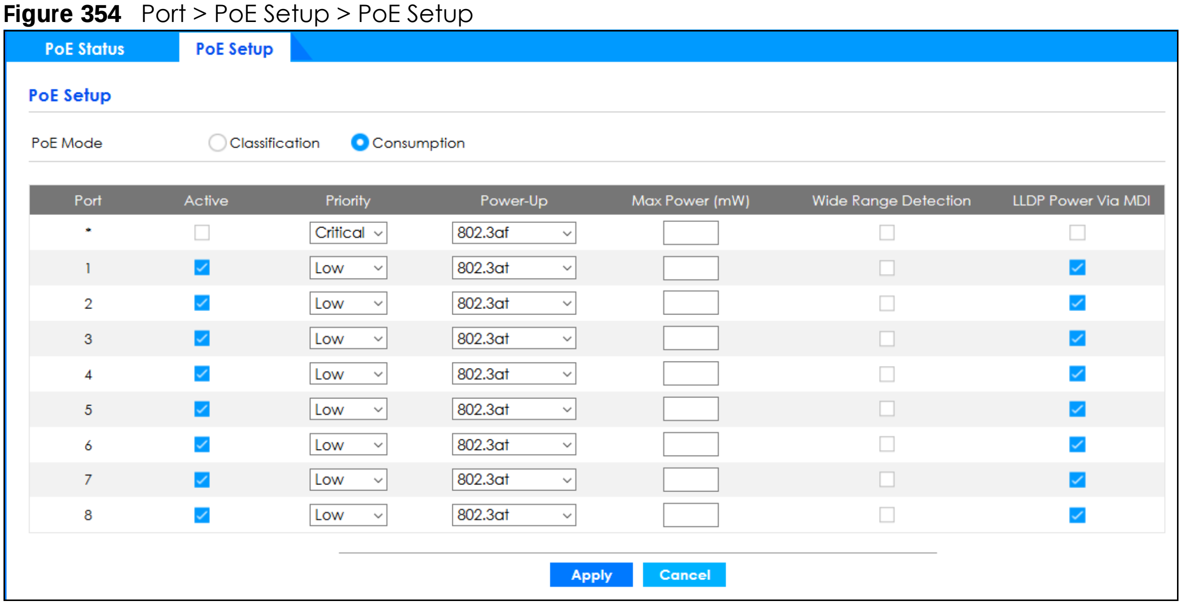
LABEL	DESCRIPTION
Class	This shows the power classification of the PD. Each PD has a specified maximum power that fall under one of the classes. The Class is a number from 0 to 4, where each value represents the range of power that the Switch provides to the PD. Each class corresponds to a default maximum power that can be extended in **Port** > **PoE Setup** > **PoE Setup** to the following values. • **Class 0** – default: 0.44 W to 15.4 W, can be extended to 17.8 W. • **Class 1** – default: 0.44 W to 4 W, can be extended to 5.8 W. • **Class 2** – default: 0.44 W to 7 W, can be extended to 9 W. • **Class 3** – default: 0.44 W to 15.4 W, can be extended to 17.8 W. • **Class 4** – default: 0.44 W to 30 W, can be extended to 32.8 W.
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	This field displays the PoE standard the Switch uses to provide power on this port.
Consuming Power (W)	This field displays the current amount of power consumed by the PD from the Switch on this port.
Max Power (W)	This field displays the maximum amount of power the PD could use from the Switch on this port.

60.3 PoE Setup

Use this screen to set the PoE power management mode, priority levels, power-up mode and the maximum amount of power for the connected PDs.

Click **Port** > **PoE Setup** > **PoE Setup**, the following screen opens.

Figure 354   Port > PoE Setup > PoE Setup



The following table describes the labels in this screen.

Table 245 Port > 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 maximum power for each PD according to the PD's power class and priority level. If the total power supply runs out, PDs with lower priority do not get power to function. In this mode, the maximum power is reserved based on what you configure in **Max Power** or the standard power limit for each class. • **Consumption** – Select this if you want the Switch to supply the actual power that the PD needs. The Switch also allocates power based on a port's **Max Power** and the PD's power class and priority level. The Switch puts a limit on the maximum amount of power the PD can request and use. In this mode, the default maximum power that can be delivered to the PD is 33 W (IEEE 802.3at Class 4) or 22 W (IEEE 802.3af Classes 0 to 3).
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	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.
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. Select **Critical** to give the highest PD priority on the port. 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	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 30 W 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. **Force-802.3at** – the Switch offers power of up to 33 W on the port without performing PoE hardware classification. Select this option if the connected PD does not comply with any PoE standard and requests power higher than a standard power limit.
Max Power (mW)	Specify the maximum amount of power the PD could use from the Switch on this port. If you leave this field blank, the Switch refers to the standard or default maximum power for each class.

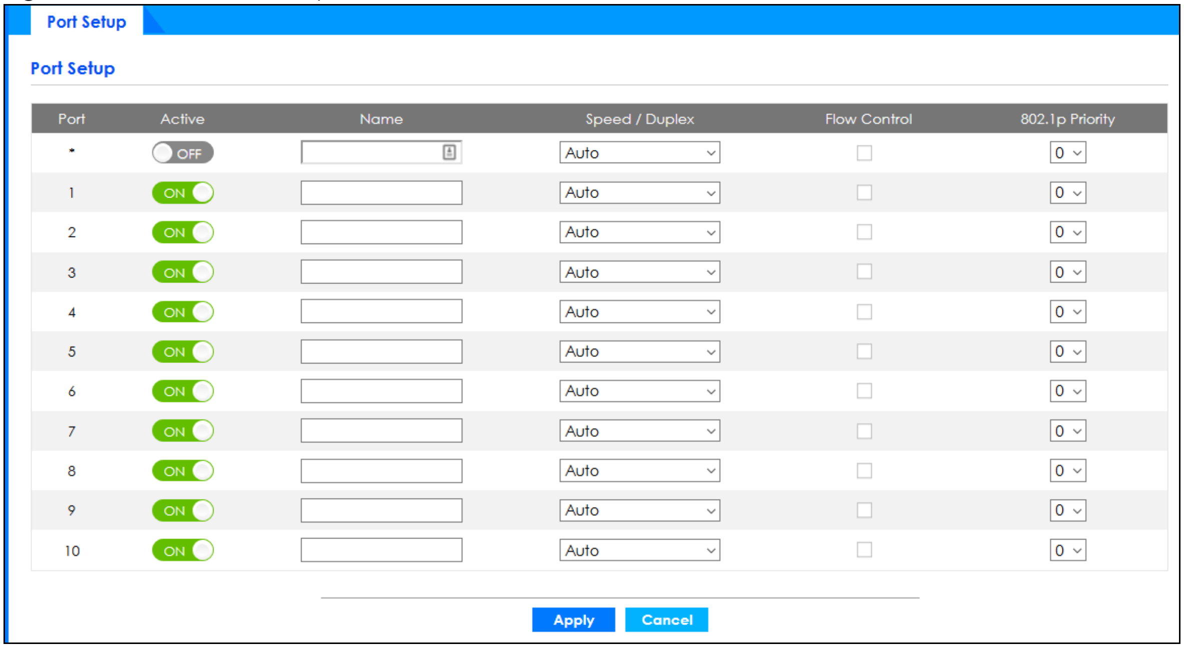
Table 245 Port > PoE Setup > PoE Setup (continued)

LABEL	DESCRIPTION
Wide Range Detection	Select this to let the Switch have a wider detection range for the PD. The Switch detects whether a connected device is a powered device or not before supplying power to the port. For the PD detection, the Switch applies a fixed voltage to the device and then receives returned current. If the returned current is within the IEEE 802.3AF/AT standard range, the device will be considered as a valid PD by the Switch. However, in real cases, environmental interferences might easily cause the returned current to be out of the standard range.
LLDP Power Via MDI	Select this to have the Switch negotiate PoE power with the PD connected to the port by transmitting LLDP Power Via MDI TLV frames. This helps the Switch allocate less power to the PD on this port. The connected PD must be able to request PoE power through LLDP. The Power Via MDI TLV allows PoE devices to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controllable • 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.

60.4 Port Setup

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

Figure 355 Port > Port Setup



The following table describes the labels in this screen.

Table 246 Port > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some Web Configurator screens.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10-an** (10M/auto-negotiation), **10M/Half Duplex**, **10M/Full Duplex**, **100-an** (100M/auto-negotiation), **100M/Half Duplex**, **100M/Full Duplex** and **1G/Full Duplex** (Gigabit connections only). 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.

Table 246 Port > Port Setup (continued)

LABEL	DESCRIPTION
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 IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x 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 26 on page 105 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.

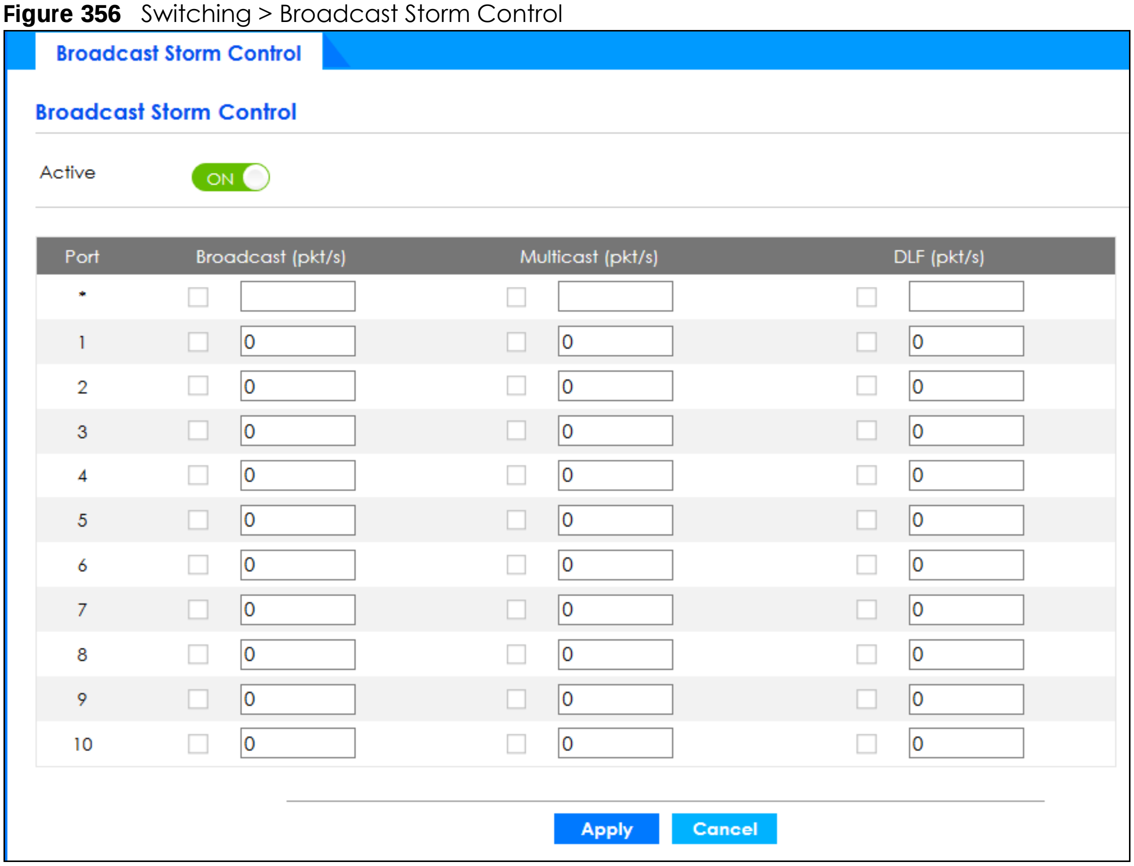
CHAPTER 61 Switching

61.1 Broadcast Storm Control

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. 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 **Switching** > **Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 356 Switching > Broadcast Storm Control



The following table describes the labels in this screen.

Table 247 Security > Broadcast Storm Control

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

61.2 Link Aggregation

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

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.

61.2.1 What You Can Do

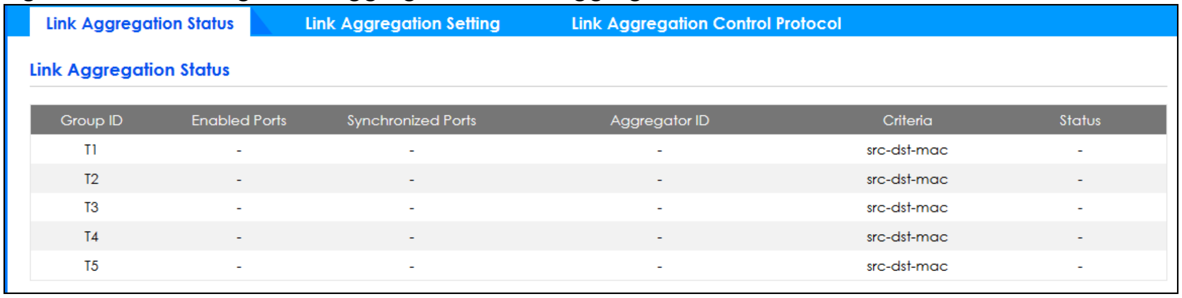
- Use the **Link Aggregation Status** screen (Section 61.3 on page 477) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen (Section 61.4 on page 478) to configure to enable static link aggregation.
- Use the **Link Aggregation Control Protocol** screen (Section 61.5 on page 480) to enable Link Aggregation Control Protocol (LACP).

61.3 Link Aggregation Status

Use the **Link Aggregation Status** screen to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.

Click **Switching** > **Link Aggregation** > **Link Aggregation Status** in the navigation panel.

Figure 357 Switching > Link Aggregation > Link Aggregation Status



The following table describes the labels in this screen.

Table 248 Switching > Link Aggregation > Link Aggregation Status

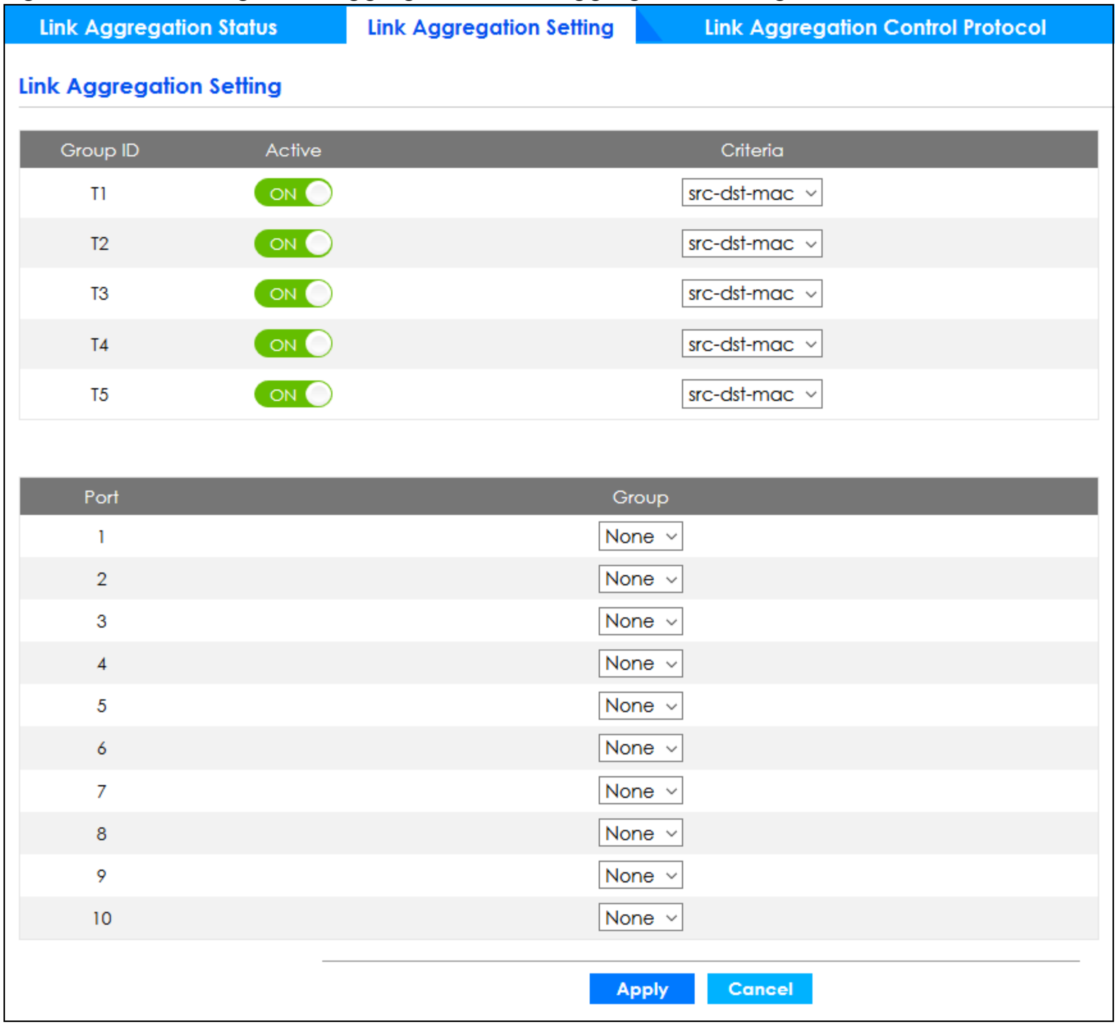
LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group. The port numbers displays only when this trunk 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. 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.

61.4 Link Aggregation Setting

Use the **Link Aggregation Setting** screen to enable static link. 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.

Click **Switching** > **Link Aggregation** > **Link Aggregation Setting** to display the screen shown next.

Figure 358 Switching > Link Aggregation > Link Aggregation Setting



The following table describes the labels in this screen.

Table 249 Switching > 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.
Active	Set this switch to on to activate a trunk group.

Table 249 Switching > Link Aggregation > Link Aggregation Setting (continued)

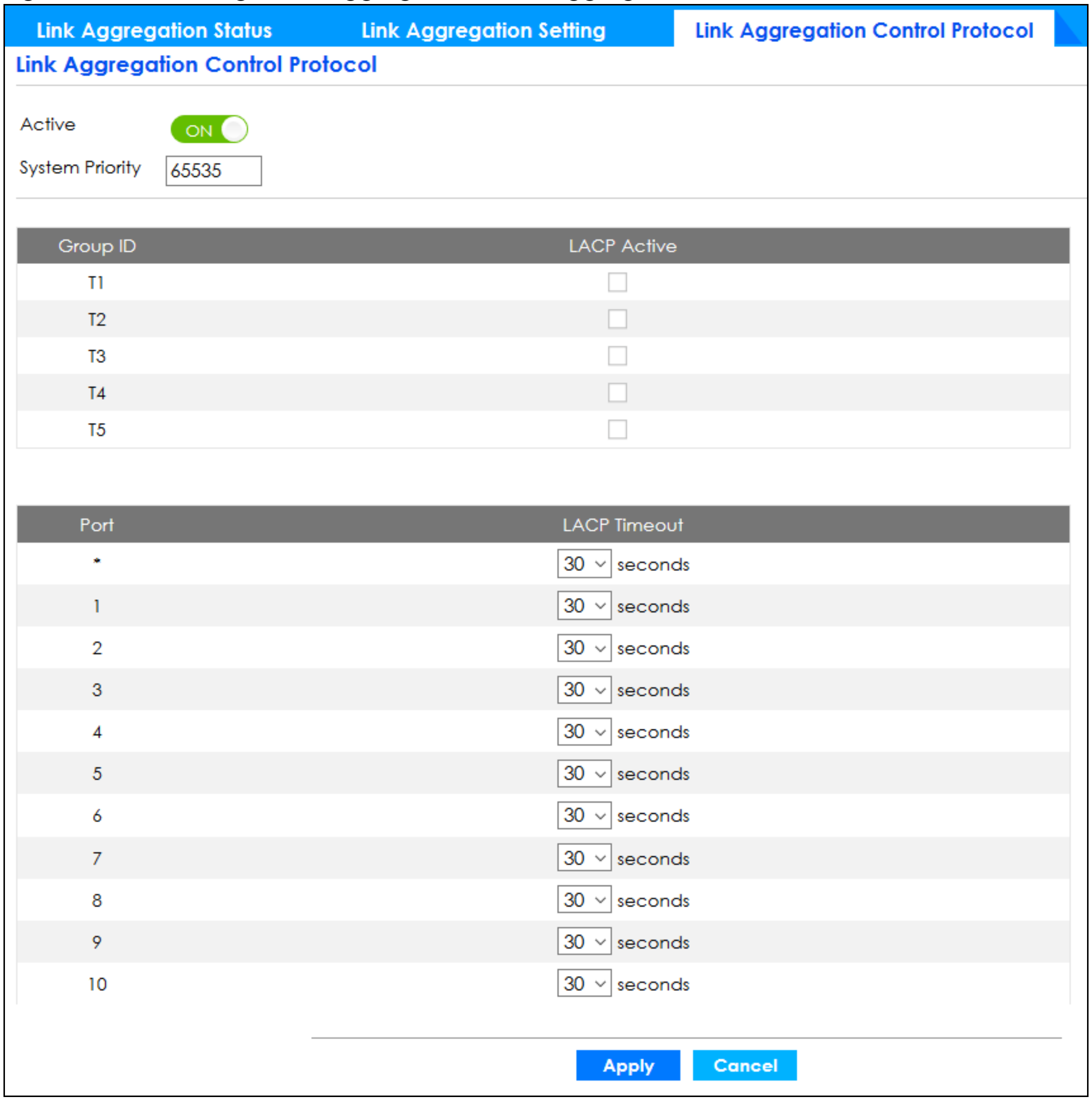
LABEL	DESCRIPTION
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **src-dst-mac** distribution type. If the Switch is behind a router, the packet's destination 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.
Port	This field displays 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.

61.5 Link Aggregation Control Protocol

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.

Click **Switching** > **Link Aggregation** > **Link Aggregation Control Protocol** to display the screen shown next.

Figure 359 Switching > Link Aggregation > Link Aggregation Control Protocol



The following table describes the labels in this screen.

Table 250 Switching > Link Aggregation > Link Aggregation Control Protocol

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do NOT configure this screen unless you want to enable dynamic link aggregation.
Active	Set this switch to **ON** to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.

Table 250   Switching > Link Aggregation > Link Aggregation Control Protocol (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.
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.

61.6 VLAN

This section shows you how to configure 802.1Q tagged and port-based VLANs.

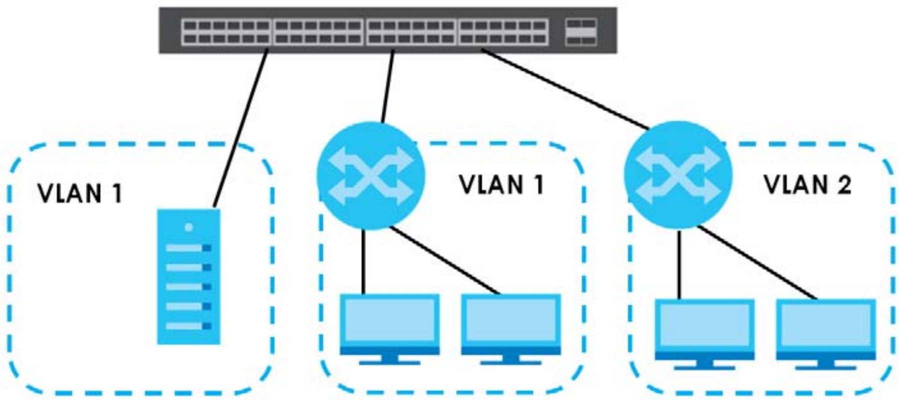
61.6.1 What You Can Do

- Use the **VLAN Status** screen (Section 61.7 on page 485) to view and search all static VLAN groups.
- Use the **VLAN Detail** screen (Section 61.7.1 on page 485) to view detailed port settings and status of the static VLAN group.
- Use the **Static VLAN** screen (Section 61.8 on page 486) to configure a static VLAN for the Switch.
- Use the **VLAN Port Setting** screen (Section 61.9 on page 488) to configure the static VLAN (IEEE 802.1Q) settings on a port.

61.6.2 What You Need to Know

Read this section to know more about VLAN and how to configure the screens.

Figure 360   Shared Server Using VLAN Example



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 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 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and 2 bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

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

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

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.

61.6.2.1 Automatic VLAN Registration

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

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.

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.

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 251 IEEE 802.1Q VLAN Terminology

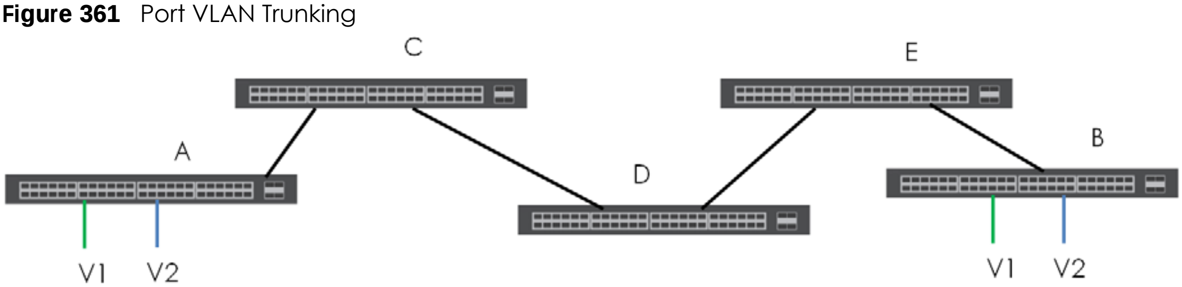
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration or de-registration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration 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 do not 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.

61.6.2.2 Port VLAN Trunking

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

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on ports 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 ports.

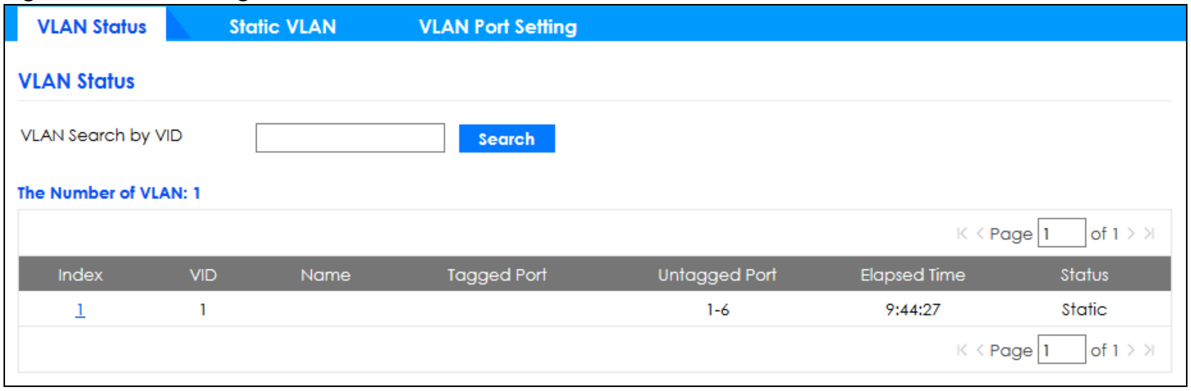
Figure 361 Port VLAN Trunking



61.7 VLAN Status

Use this screen to view and search all static VLAN groups. Click **Switching** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 362 Switching > VLAN: VLAN Status



The following table describes the labels in this screen.

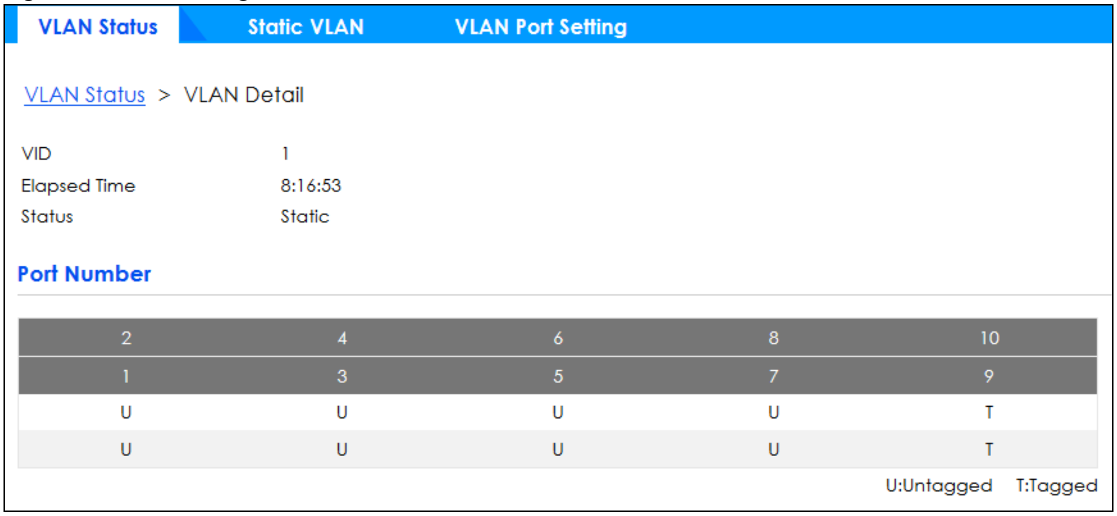
Table 252 Switching > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID numbers (separated by a comma) and click **Search** to display only the specified VLANs 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 corresponding VLAN configuration screen.
Name	This fields shows the descriptive name of the VLAN.
Tagged Port	This field shows the tagged ports that are participating in the VLAN.
Untagged Port	This field shows the untagged ports that are participating in the VLAN.
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. **Static**: added as a permanent entry.
Page	Click the forward or back icon to show the previous or next screen if all status information cannot be seen in one screen. Or enter the page number.

61.7.1 VLAN Detail

Use this screen to view detailed port settings and status of the static VLAN group. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 363 Switching > VLAN > VLAN Status > VLAN Detail



The following table describes the labels in this screen.

Table 253 Switching > VLAN > VLAN Status > 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 corresponding VLAN configuration 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. **Static**: added as a permanent entry.
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 "**–**".

61.8 Static VLAN

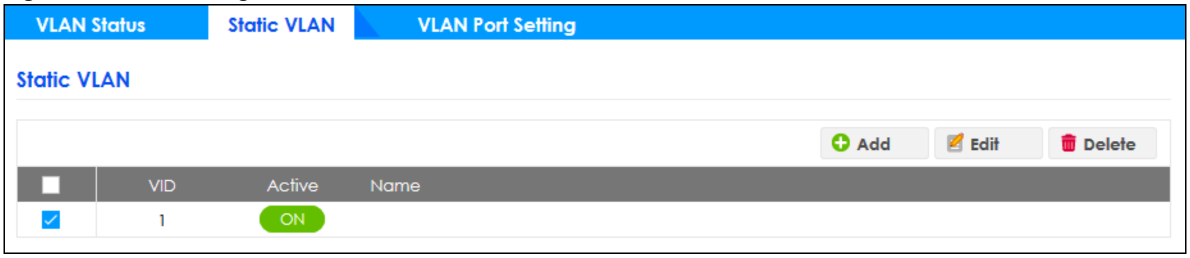
Use a static VLAN to decide whether an incoming frame on a port should be

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

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

Use this screen to view static VLAN status for the Switch. Click **Switching** > **VLAN** > **Static VLAN** to display the screen as shown next.

Figure 364 Switching > VLAN > Static VLAN



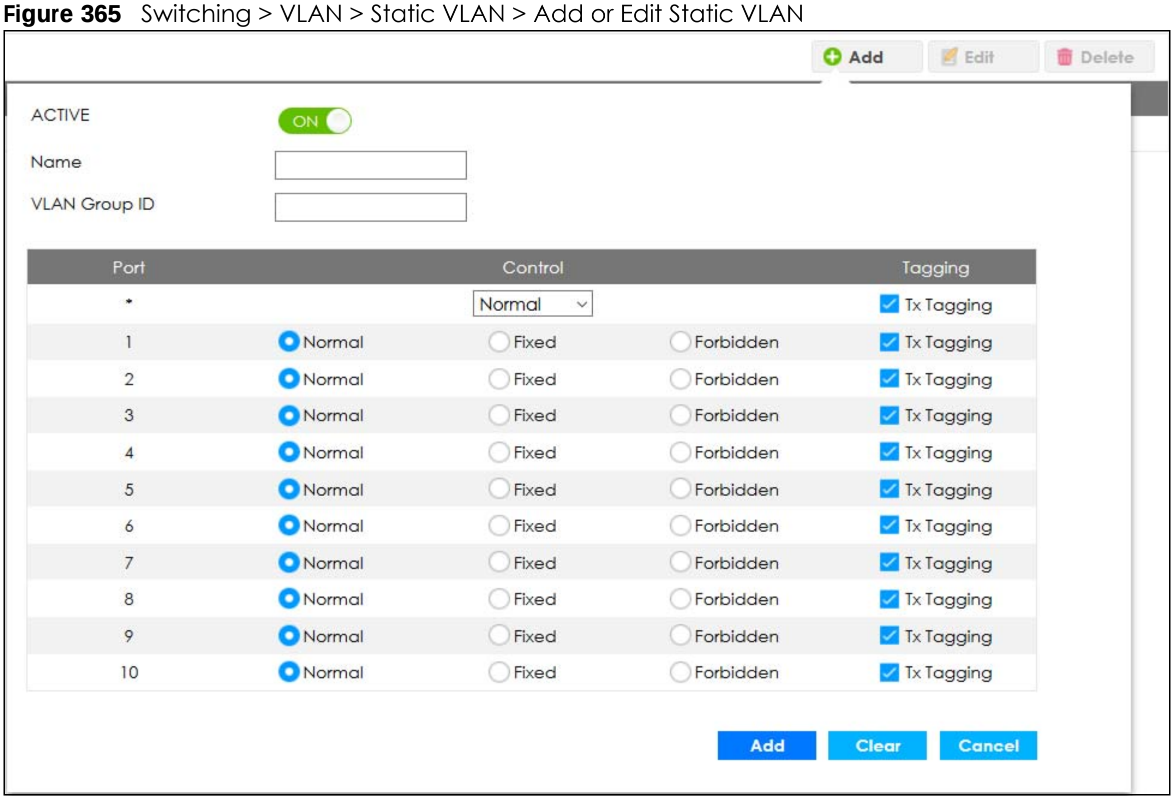
The following table describes the related labels in this screen.

Table 254 Switching > VLAN > Static VLAN

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.
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 (**ON**) or disabled (**OFF**).
Name	This field displays the descriptive name for this VLAN group.
Add	Click this button to create a new static VLAN.
Edit	Click this button to configure the static VLAN.
Delete	Click this button to remove the static VLAN.

Click **Add** or **Edit** button to open the following screen. Use this screen to configure a static VLAN for the Switch.

Figure 365 Switching > VLAN > Static VLAN > Add or Edit Static VLAN



The following table describes the related labels in this screen.

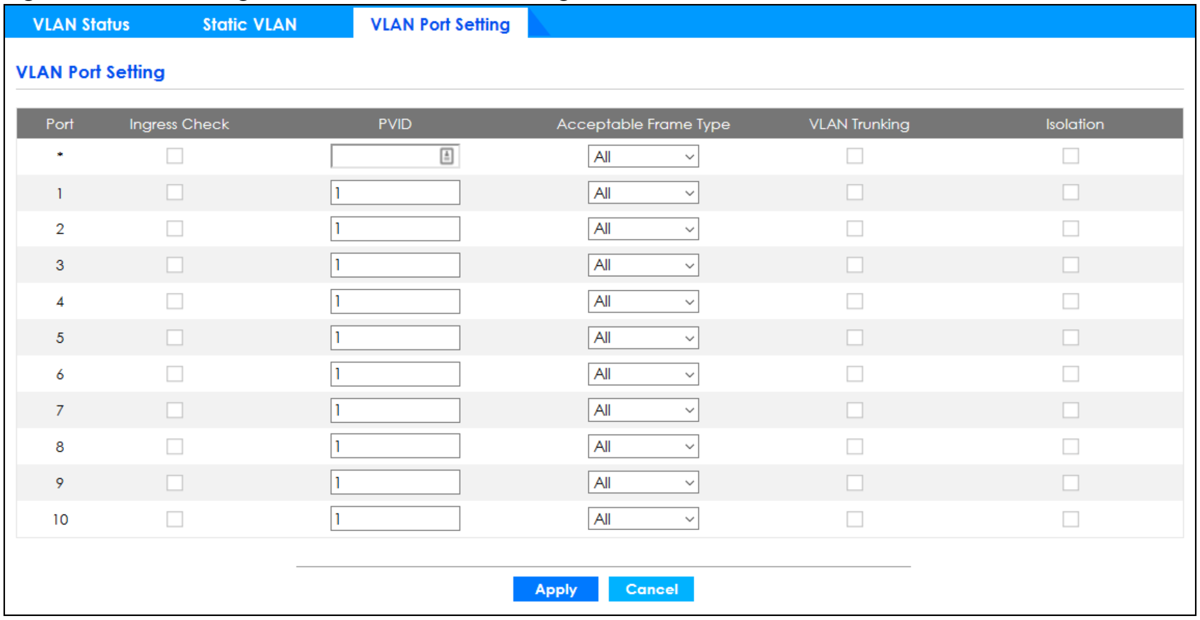
Table 255   Switching > VLAN > Static VLAN > Add or Edit Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this switch 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.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select **Normal** for the port to dynamically join this VLAN group. 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 outgoing traffic to contain this VLAN tag. Otherwise, to ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.
Add/Edit	Click **Add** or **Edit** 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.
Clear	Click **Clear** to reset the fields to the factory defaults.
Cancel	Click **Cancel** to change the fields back to their last saved values.

61.9 VLAN Port Setting

Use this screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click the **VLAN Port Setting** tab in the **VLAN** screen.

Figure 366 Switching > VLAN > VLAN Port Setting



The following table describes the labels in this screen.

Table 256 Switching > VLAN > VLAN Port Setting

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. 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, the Switch discards incoming frames on a port 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 1and 4094 as the port VLAN ID.
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.
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.

61.10 Multicast

Traditionally, IP packets are transmitted in one of either two ways – Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group – it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

This section shows you how to configure various multicast features.

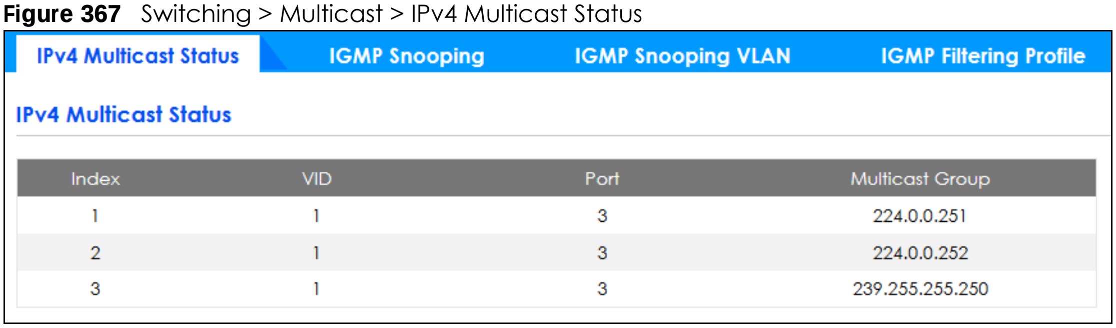
61.10.1 What You Can Do

- Use the **IPv4 Multicast Status** screen (Section 61.11 on page 490) to view multicast group information.
- Use the **IGMP Snooping** screen (Section 61.12 on page 491) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IGMP Snooping VLAN** screen (Section 61.13 on page 494) to perform IGMP snooping on up to 16 VLANs.
- Use the **IGMP Filtering Profile** screen (Section 61.14 on page 496) to specify a range of multicast groups that clients connected to the Switch are able to join.

61.11 IPv4 Multicast Status

Use this screen to view the IPv4 multicast group information. Click **Switching** > **Multicast** from the navigation panel to display the **IPv4 Multicast Status** screen as shown next.

Figure 367 Switching > Multicast > IPv4 Multicast Status



The following table describes the labels in this screen.

Table 257 Switching > Multicast > IPv4 Multicast Status

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.
Multicast Group	This field displays IP multicast group addresses.

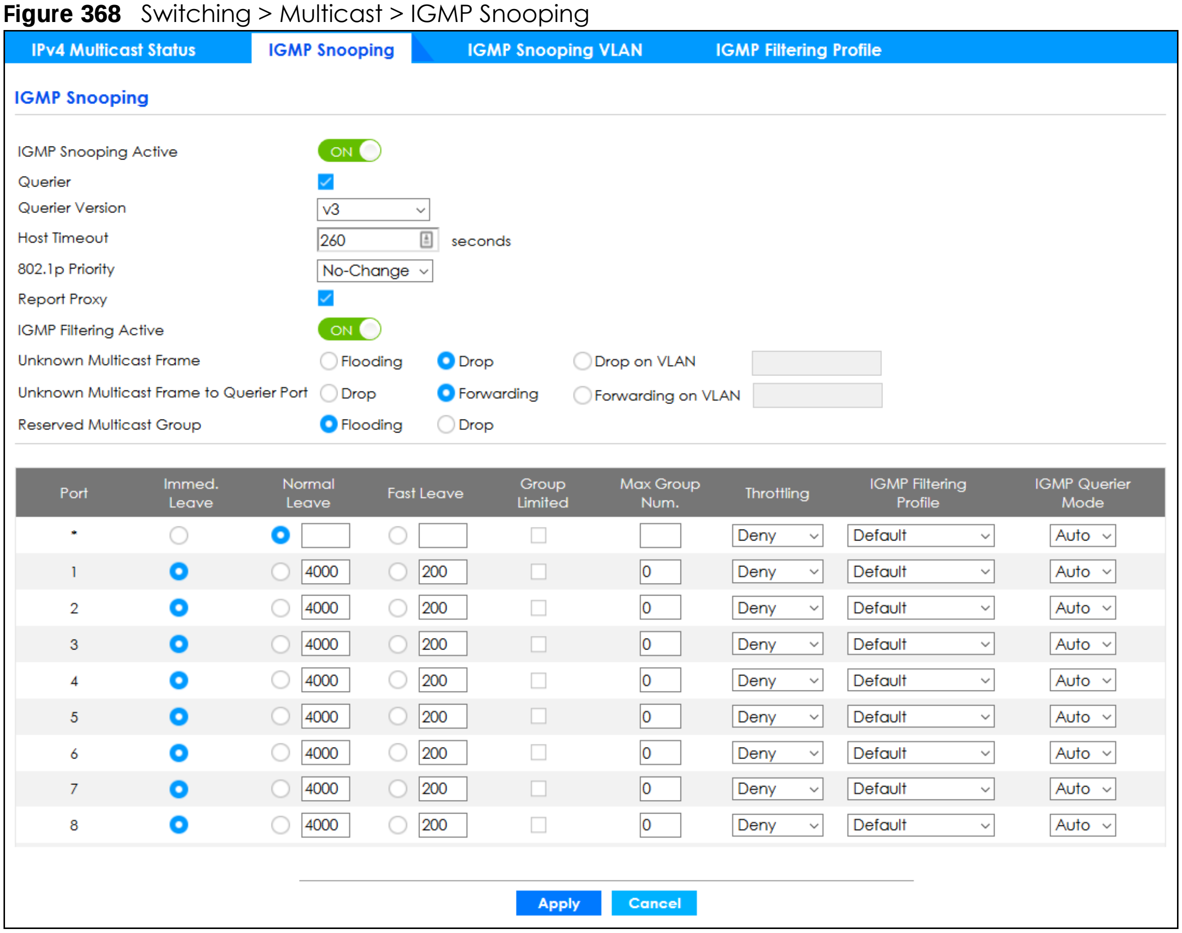
61.12 IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers or 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.

Click the **IGMP Snooping** link in the **Switching** > **Multicast** screen to display the screen as shown.

Figure 368 Switching > Multicast > IGMP Snooping



The following table describes the labels in this screen.

Table 258 Switching > Multicast > IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP snooping.
Active	Select **ON** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.

Table 258 Switching > Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Querier	IGMP Snooping Querier is used in the absence of an IP multicast router. For example, in a network where IP multicast is configured, the IP multicast router acts as the IGMP Snooping Querier. If the multicast traffic in a VLAN only needs to be Layer 2 switched, an IP multicast router is NOT required. But without an IP multicast router on the VLAN, you must configure the Switch as the IGMP Snooping Querier so that it can send queries. Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Querier Version	IGMP snooping query works only when both host and Switch support the same IGMP version. Select **v2** to allow the Switch to send IGMPv2 queries only. Select **v3** to allow the Switch to send IGMPv3 queries only.
Host Timeout	Specify the time (from 1 to 16711450) 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.
Report Proxy	Select this option to allow the Switch to act as the IGMP report proxy and leave proxy. It will report group changes to a connected multicast router. The Switch not only checks IGMP packets between multicast routers or switches and multicast hosts to learn the multicast group membership, but also replaces the source MAC address in an IGMP v1/v2 report with its own MAC address before forwarding to the multicast router or switch. When the Switch receives more than one IGMP v1/v2 join report that requests to join the same multicast group, it only sends a new join report with its MAC address. This helps reduce the number of multicast join reports passed to the multicast router or switch. The Switch sends a leave message with its MAC address to the multicast router or switch only when it receives the leave message from the last host in a multicast group.
IGMP Filtering Active	Select **On** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. 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 frames. • Select **Flooding** to send the frames to all ports. • Select **Drop on VLAN** and enter the VLAN ID numbers to discard the frames on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
Unknown Multicast Frame to Querier Port	Specify the action to perform when **Unknown Multicast Frame** is set to **Drop**. • Select **Drop** to discard the frames. • Select **Forwarding** to send the frames to all querier ports. • Select **Forwarding on VLAN** and enter the VLAN ID numbers to send the frames to the ports which are used as an IGMP query port on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.

Table 258 Switching > Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
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 frames. • Select **Flooding** to send the frames to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. 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.
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6348800) 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 6348800) 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 frames 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 reports received on this port.

Table 258   Switching > Multicast > IGMP Snooping (continued)

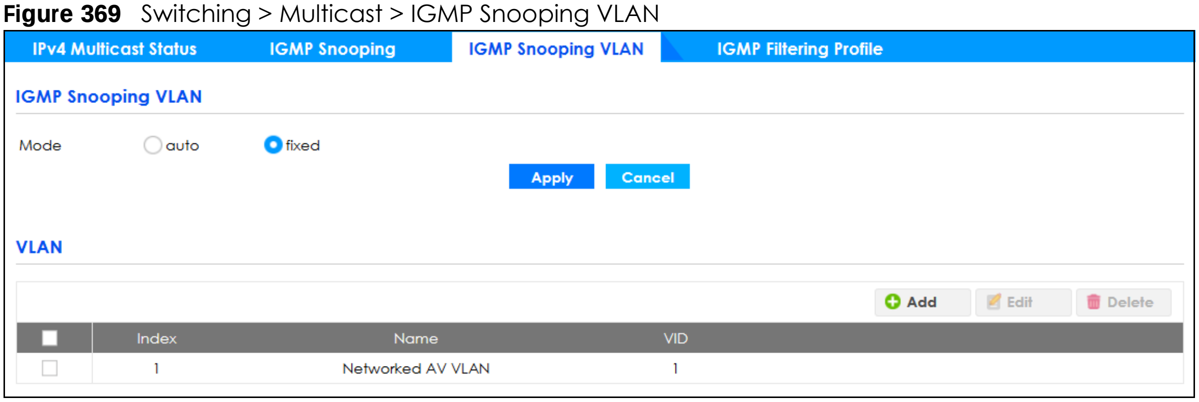
LABEL	DESCRIPTION
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the **Switching** > **Multicast** > **IGMP Filtering Profile** screen.
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.

61.13 IGMP Snooping VLAN

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.

Click **Switching** > **Multicast** in the navigation panel. Click the **IGMP Snooping VLAN** tab to display the screen as shown.

Figure 369   Switching > Multicast > IGMP Snooping VLAN



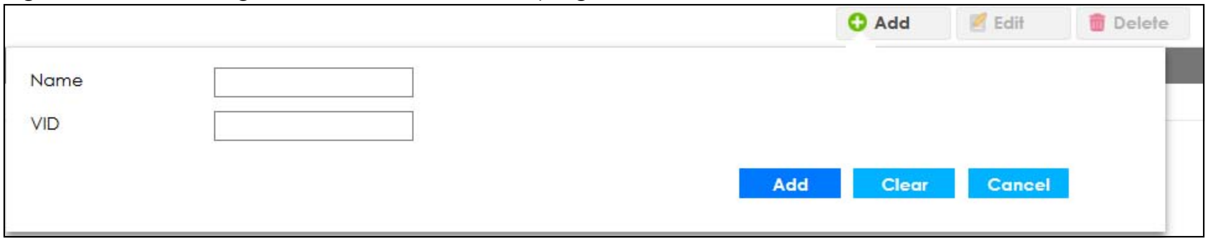
The following table describes the labels in this screen.

Table 259 Switching > Multicast > 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 VLANs that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. You must also enable IGMP snooping in the **Switching** > **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 view and add or edit VLANs upon which the Switch is to perform IGMP snooping.
	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.
Index	This is the index number of the IGMP snooping VLAN entry in the table. Click on an index number to view more details or change the settings.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Add Edit	Click **Add** to create a new entry or **Edit** 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.
Delete	Check the entries that you want to remove, then click the **Delete** button.

Click **Add** or **Edit** button to open the following screen. Use this screen to configure a static VLAN for the Switch.

Figure 370 Switching > Multicast > IGMP Snooping VLAN > Add or Edit VLAN



The following table describes the related labels in this screen.

Table 260 Switching > Multicast > IGMP Snooping VLAN > Add or Edit VLAN

LABEL	DESCRIPTION
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.
Add/Edit	Click **Add** or **Edit** 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.

Table 260   Switching > Multicast > IGMP Snooping VLAN > Add or Edit VLAN (continued)

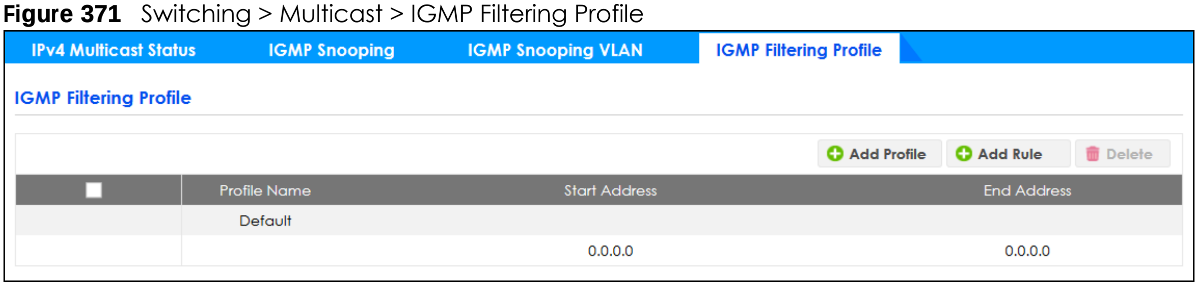
LABEL	DESCRIPTION
Clear	Click **Clear** to have the fields display blanks.
Cancel	Click **Cancel** to change the fields back to their last saved values.

61.14 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 **Switching** > **Multicast** in the navigation panel. Click the **IGMP Filtering Profile** tab to display the screen as shown.

Figure 371   Switching > Multicast > IGMP Filtering Profile



The following table describes the labels in this screen.

Table 261   Switching > Multicast > IGMP Filtering Profile

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.
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.
Add Profile	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.
Add Rule	Click this to create a new rule for a profile.
Delete	To delete the profiles and all the accompanying rules, select the profiles that you want to remove in the corresponding row, then click the **Delete** button. To delete a rule from a profile, select the rule that you want to remove in the corresponding row, then click the **Delete** button.

Click the **Add Profile** button to open the following screen. Use this screen to configure an IGMP filtering profile for the Switch.

Figure 372 Switching > Multicast > IGMP Filtering Profile > Add Profile

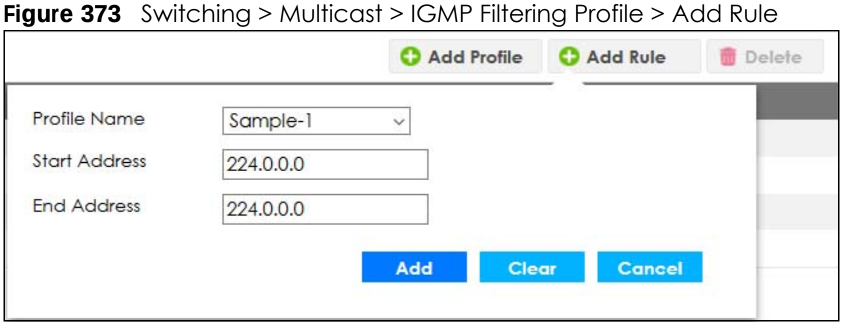
The following table describes the related labels in this screen.

Table 262 Switching > Multicast > IGMP Filtering Profile > Add Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rules for a profile that you have already added, select 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 have the fields display blanks.
Cancel	Click **Cancel** to leave this screen.

Click the **Add Rule** button to open the following screen. Use this screen to configure a rule for an IGMP filtering profile.

Figure 373 Switching > Multicast > IGMP Filtering Profile > Add Rule



The following table describes the related labels in this screen.

Table 263 Switching > Multicast > IGMP Filtering Profile > Add Rule

LABEL	DESCRIPTION
Profile Name	Select the profile name to add a rule. To configure additional rules for a profile that you have already added, select 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 have the fields display blanks.
Cancel	Click **Cancel** to leave this screen.

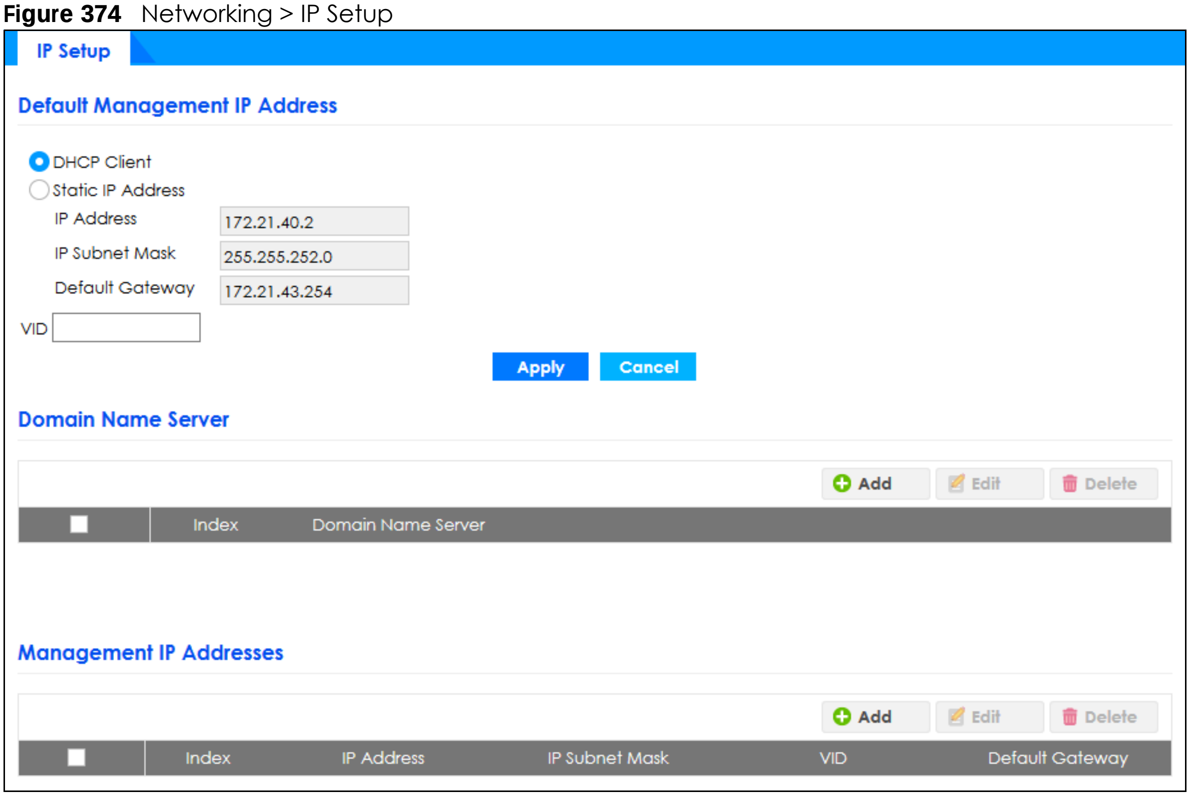
Chapter 62 Networking

This section shows you how to configure the default gateway device, the default domain name server and add IP domains.

62.1 IP Setup

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

Figure 374 Networking > IP Setup



The following table describes the labels in this screen.

Table 264 Networking > IP Setup

LABEL	DESCRIPTION
Default Management IP Address 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 do not 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, 172.21.40.x. 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, 255.255.252.0.
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 172.21.43.254.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
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.
Domain Name Server Use these fields to add, edit, or delete the IP address of the DNS 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.
Index	This field displays the index number of an entry.
Domain Name Server	This field displays the IP address of the DNS server.
Add	Click this button to create a new IP address for the DNS server.
Edit	Click this button to configure the IP address of the DNS server.
Delete	Click this button to remove the IP address of the DNS server.
Management IP Address Use these fields to set the settings for the management port.	
	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.
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.
Default Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation.
Add	Click this button to create new settings for the management port.
Edit	Click this button to configure the settings for the management port.
Delete	Click this button to remove the settings for the management port.

CHAPTER 63 Security

63.1 Access Control

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 265 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to 9 sessions		One session	Up to 5 accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the CLI Reference Guide for more information on disabling multi-login.

This section describes how to control access to the Switch.

63.1.1 What You Can Do

- Use the **Logins** screen (Section 63.2 on page 501) to assign which users can access the Switch via Web Configurator at any one time.
- Use the **Remote Management** screen (Section 63.3 on page 503) to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
- Use the **SNMP** screen (Section 63.4 on page 504) to configure your SNMP settings.
- Use the **Service Access Control** screen (Section 63.8 on page 510) to decide what services you may use to access the Switch.

63.2 Set Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via Web Configurator at any one time.

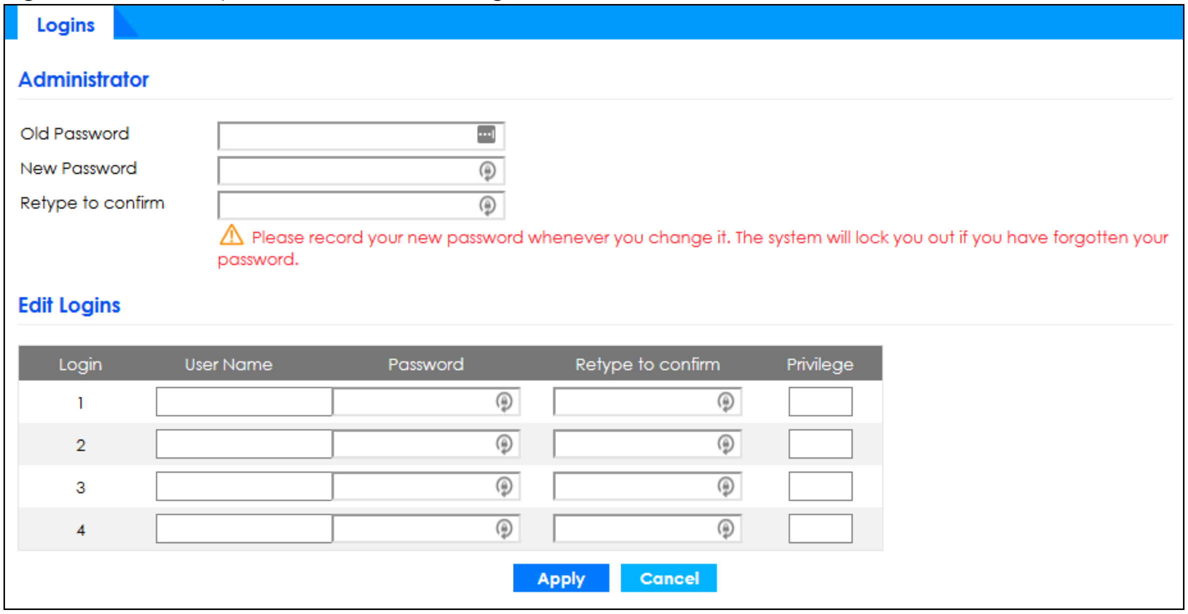
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

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 and/or configure Switch settings. The configuration right varies depending on the user's privilege level.

Click **Security** > **Access Control** > **Logins** to view the screen as shown.

Figure 375 Security > Access Control > Logins



The following table describes the labels in this screen.

Table 266 Security > 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.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation.
Edit Logins You may configure passwords for up to four users. These users can have read-only or read/write access. You can give users higher privileges via the Web Configurator or the CLI. For more information on assigning privileges via the CLI see the Ethernet Switch CLI Reference Guide.	
Login	This field displays the index number of an entry.
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 or she can run commands that requires privilege level of 5 or less but not more.

Table 266 Security > Access Control > Logins (continued)

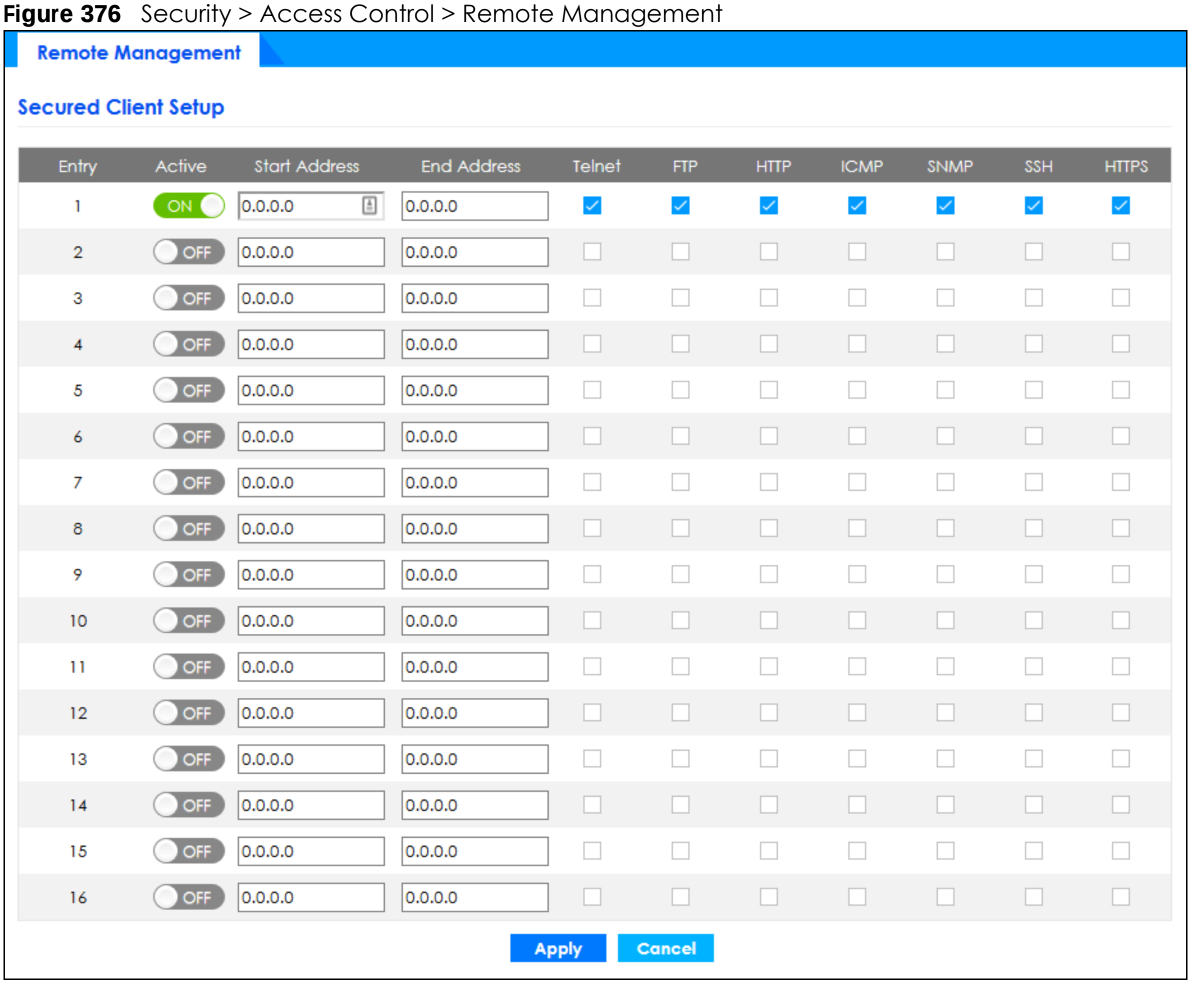
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click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

63.3 Remote Management

Use this screen to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

Click **Security** > **Access Control** > **Remote Management** to view the screen as shown next.

Figure 376 Security > Access Control > Remote Management



The following table describes the labels in this screen.

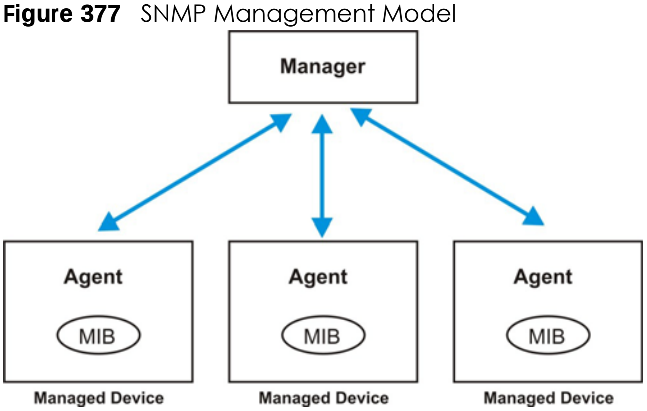
Table 267 Security > Access Control > Remote Management

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	Set this switch to **ON** 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.

63.4 Configure SNMP

Use this screen to configure your SNMP settings. 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 377 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 or 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 or response protocol based on the manager or agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 268 SNMP Commands

LABEL	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.

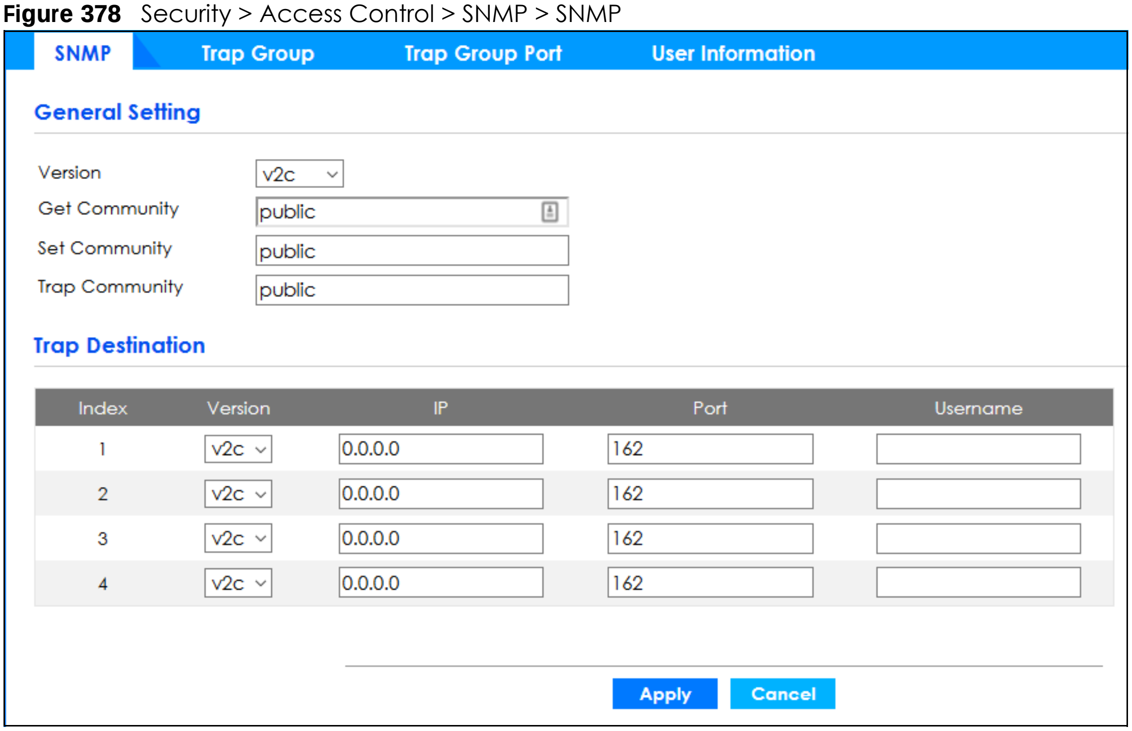
SNMP v3 and Security

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.

Click **Security** > **Access Control** > **SNMP** > **SNMP** to view the screen as shown.

Figure 378 Security > Access Control > SNMP > SNMP



The following table describes the labels in this screen.

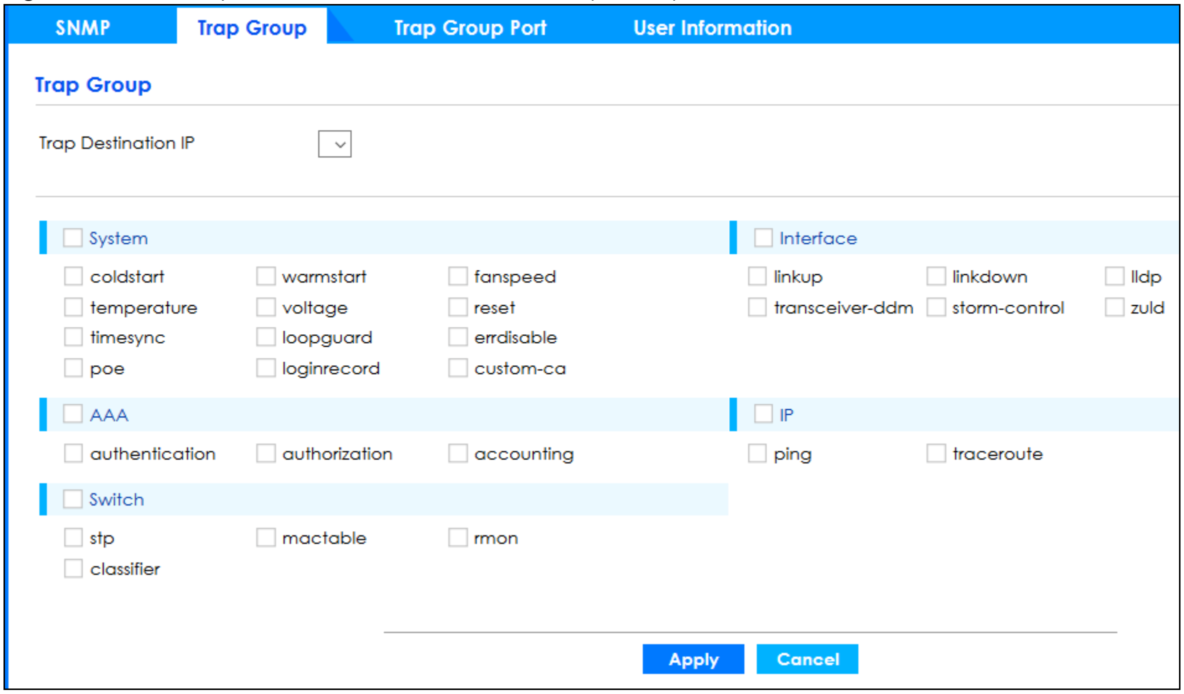
Table 269 Security > Access Control > SNMP > SNMP

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**). 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**, which is the password for 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.
Index	This field displays the index number of an entry.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to 4 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. This username must match an existing account on the Switch (configured in the **Security** > **Access Control** > **SNMP** > **User Information** 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.

63.5 Configure SNMP Trap Group

The Switch sends traps to an SNMP manager when an event occurs. 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 379 Security > Access Control > SNMP > Trap Group



The following table describes the labels in this screen.

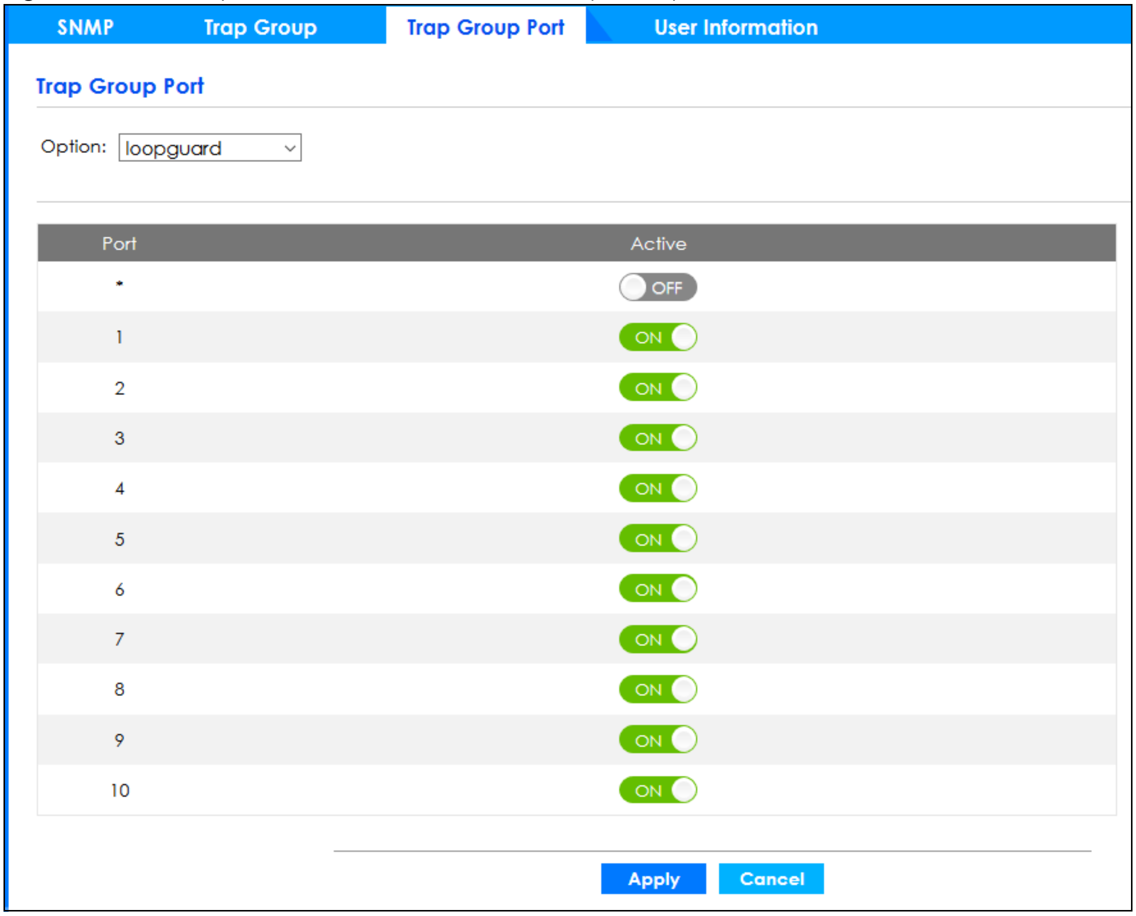
Table 270 Security > Access Control > SNMP > Trap Group

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** screen. Use the rest of the screen to select the following: • Categories of SNMP traps that the Switch is to send to the SNMP manager. • Individual SNMP traps that the Switch is to send to the SNMP station. 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.

63.6 Enable or Disable Sending of SNMP Traps on a Port

Click **Security** > **Access Control** > **SNMP** > **Trap Group Port** to view the screen as shown. Use this screen to set whether a trap received on the ports would be sent to the SNMP manager.

Figure 380 Security > Access Control > SNMP > Trap Group Port



The following table describes the labels in this screen.

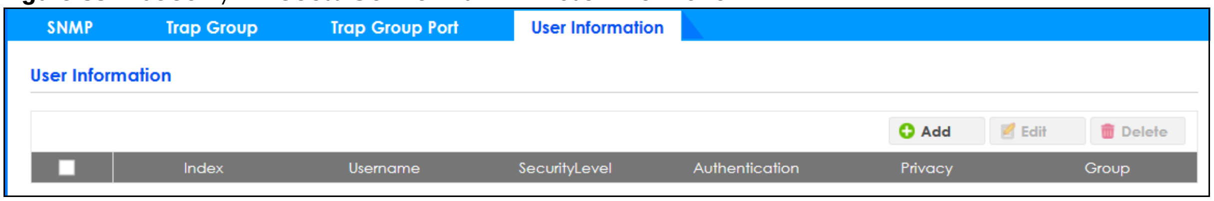
Table 271 Security > Access Control > SNMP > Trap Group Port

LABEL	DESCRIPTION
Option	Select the trap type you want to configure here.
Port	This field displays a 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. Changes in this row are copied to all the ports as soon as you make them.
Active	Set this switch to **ON** to enable the trap type of SNMP traps on this port. Set this switch to **OFF** 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.

63.7 Configure SNMP User

From the **SNMP** screen, click **User Information** to view the screen as shown. Use the **User Information** screen to view SNMP users for authentication with managers using SNMPv3 and SNMPv2c. An SNMP user is an SNMP manager.

Figure 381 Security > Access Control > SNMP > User Information



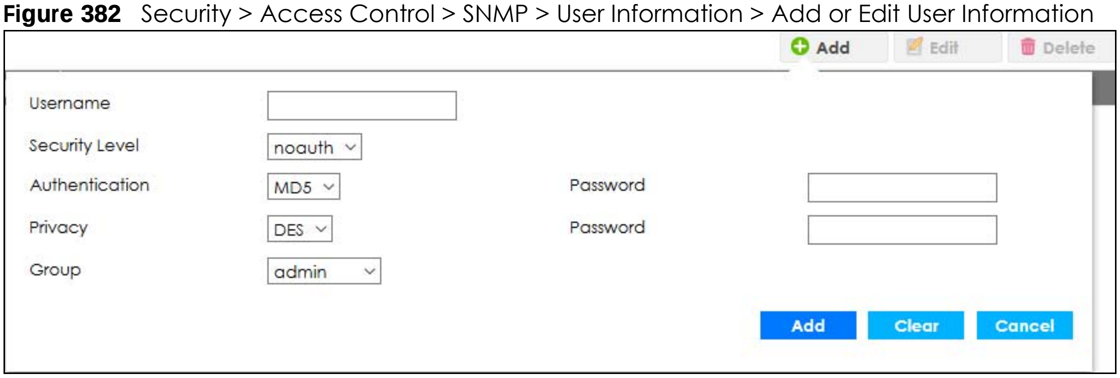
The following table describes the labels in this screen.

Table 272 Security > Access Control > SNMP > User Information

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.
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.
Add	Click this button to create new SNMP users for authentication with managers.
Edit	Click this button to configure SNMP users for authentication with managers.
Delete	Click this button to remove the selected entry from the summary table.

Click **Add** or **Edit** button to open the following screen. Use this screen to create or edit SNMP users for authentication with managers using SNMPv3 or SNMPv2c and associate them to SNMP groups.

Figure 382 Security > Access Control > SNMP > User Information > Add or Edit User Information



The following table describes the labels in this screen.

Table 273 Security > Access Control > SNMP > User Information > Add or Edit User Information

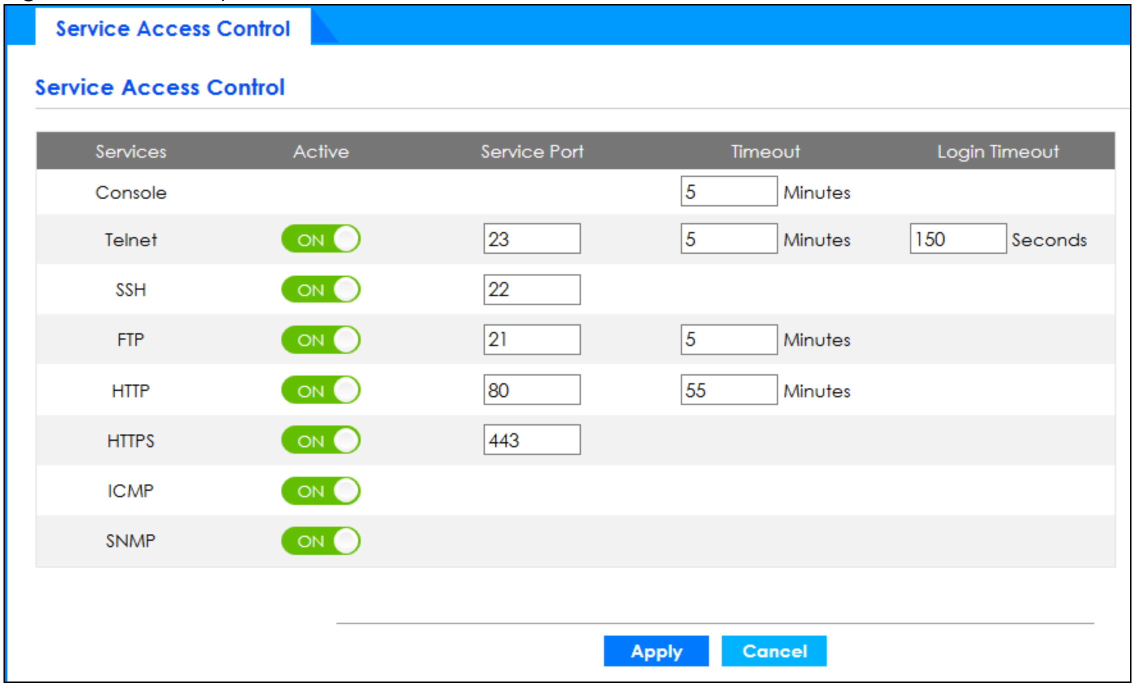
LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMPv3 or SNMPv2c manager.
Username	Specify the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • **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 SNMPv2c. 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	SNMPv3 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.
Clear	Click **Clear** to reset the fields to the factory defaults.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

63.8 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 computers" for each service in the **Remote**

Management screen (discussed earlier). Click **Security** > **Access Control** > **Service Access Control** to view the screen as shown.

Figure 383 Security > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 274 Security > 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	Enter 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.
Login Timeout	The Telnet or SSH server do not allow multiple user logins at the same time. Enter how many seconds (from 30 to 300 seconds) a login session times out. After it times out you have to start the login session again. Very long login session timeouts may have security risks. For example, if User A attempts to connect to the Switch (via SSH), but during the login stage, do not enter the user name and/or password, User B cannot connect to the Switch (via SSH) before the **Login Timeout** for User A expires (default 150 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.

CHAPTER 64 Maintenance

This section explains how to configure the screens that let you maintain the firmware and configuration files.

64.1 What You Can Do

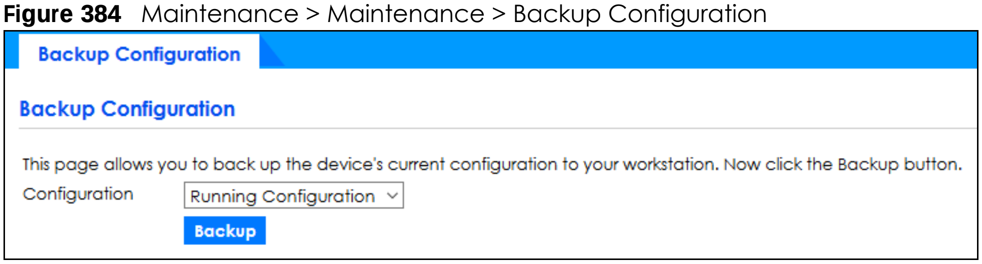
- Use the **Backup Configuration** screen (Section 64.2 on page 512) to save your configuration for later use.
- Use the **Firmware Upgrade** screen (Section 64.3 on page 513) to upload the latest firmware.
- Use the **Reboot System** screen (Section 64.4 on page 514) to restart the Switch without physically turning the power off and load a specific configuration file.
- Use the **Restore Configuration** screen (Section 64.5 on page 515) to upload a stored device configuration file.
- Use the **Save Configuration** screen (Section 64.6 on page 515) to save the current configuration settings to a specific configuration file on the Switch.
- Use the **Tech-Support** screen (Section 64.7 on page 516) to create reports for customer support if there are problems with the Switch.

64.2 Backup Configuration

Backing up your Switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Click **Maintenance** > **Maintenance** > **Backup Configuration** to display the screen as shown next. Use this screen to back up your current Switch configuration and log files to a server or as local files to your computer.

Figure 384 Maintenance > Maintenance > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Choose the type of configuration files for backup (running, current, and custom default).

2 Click **Backup**.

3 If a dialog box pops up asking whether you want to open or save the file, click **Save File** to download it to the default downloads folder on your computer. Click **OK** to save the configuration file to your computer.

64.3 Firmware Upgrade

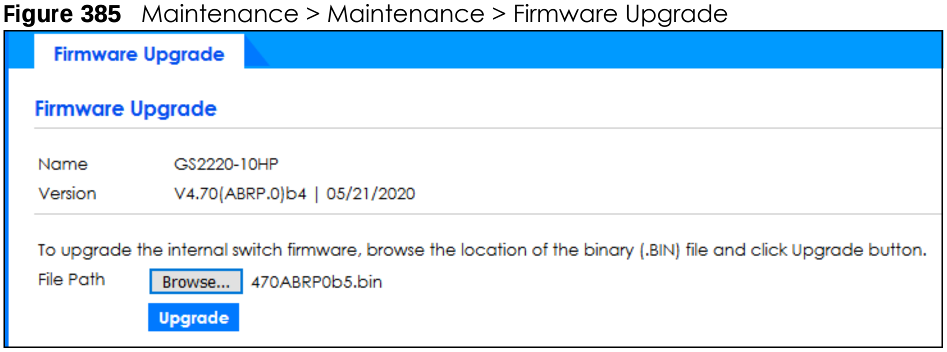
Use the following screen to upgrade your Switch to the latest firmware.

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.

Click **Maintenance** > **Maintenance** > **Firmware Upgrade** to view the screen as shown next.

Figure 385 Maintenance > Maintenance > Firmware Upgrade



Click **Choose File** or **Browse** to locate the firmware file you wish to upload to the Switch. Firmware upgrades are only applied after a reboot. Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

Table 275 Maintenance > Maintenance > Firmware Upgrade

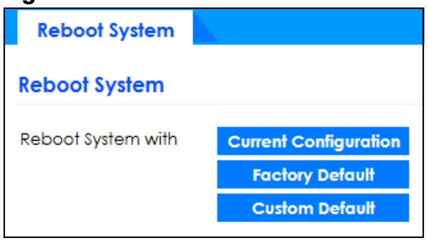
LABEL	DESCRIPTION
Name	This is the name of the Switch that you are configuring.
Version	This is the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch. The firmware information is also displayed in **System** > **System Information**.
File Path	Enter the path and file name of the firmware file you wish to upload to the Switch in the **File Upload** text box or click **Choose File** or **Browse** to locate it.
Upgrade	Click **Upgrade** to load the new firmware. Firmware upgrades are only applied after a reboot. To reboot, go to **Maintenance** > **Maintenance** > **Reboot System** and click **Current Configuration**, **Factory Default**, or **Custom Default** (**Current Configuration**, **Factory Default**, and **Custom Default** are the configuration files you want the Switch to use when it restarts).

64.4 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load the **Current Configuration**, a **Custom Default** or the **Factory Default** configuration when you reboot. Follow the steps below to reboot the Switch.

Click **Maintenance** > **Maintenance** > **Reboot System** to view the screen as shown next.

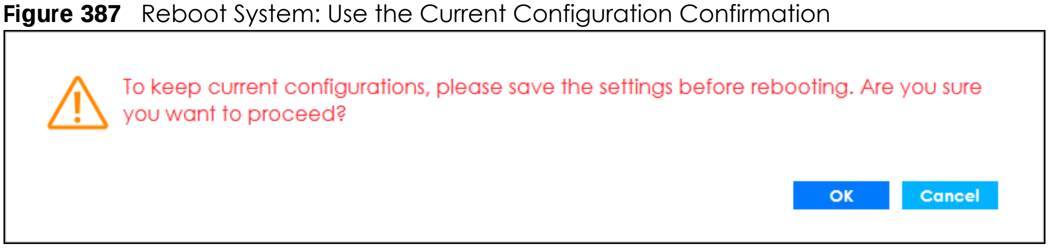
Figure 386 Maintenance > Maintenance > Reboot System



1 In the **Reboot System** screen, click a configuration button next to **Reboot System with** to reboot and load that configuration file. The following screen displays.

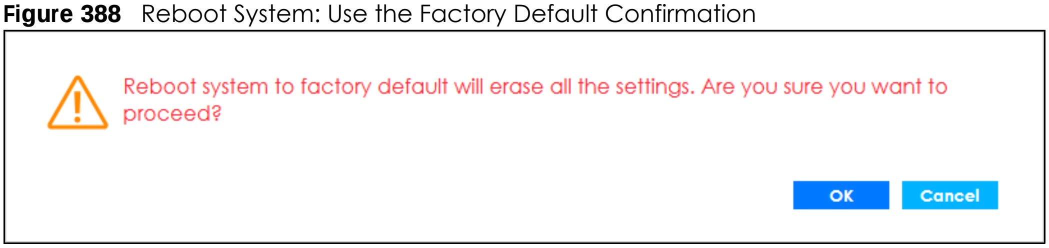
If you select **Current Configuration**, make sure to save the Switch settings as the current configuration in the **Maintenance** > **Maintenance** > **Save Configuration** screen.

Figure 387 Reboot System: Use the Current Configuration Confirmation



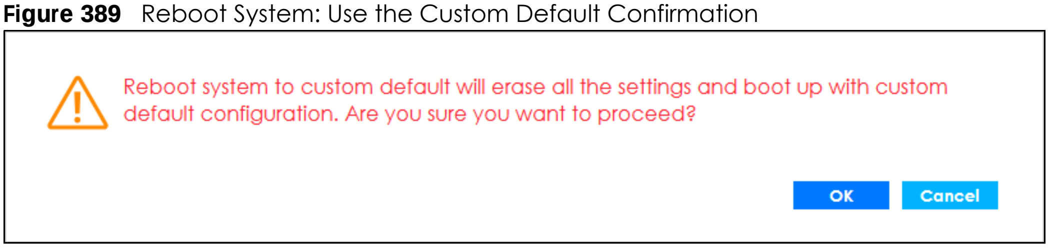
If you select **Factory Default**, the following warning will appear.

Figure 388 Reboot System: Use the Factory Default Confirmation



If you select **Custom Default**, the following warning will appear.

Figure 389 Reboot System: Use the Custom Default Confirmation



2 Click **OK** again and then wait for the Switch to restart. This takes up to 2 minutes. This does not affect the Switch's configuration.

Click **Current Configuration** and follow steps 1 to 2 to reboot and load the current configuration on the Switch.

Click **Factory Default** and follow steps 1 to 2 to reboot and load Zyxel factory default configuration settings on the Switch.

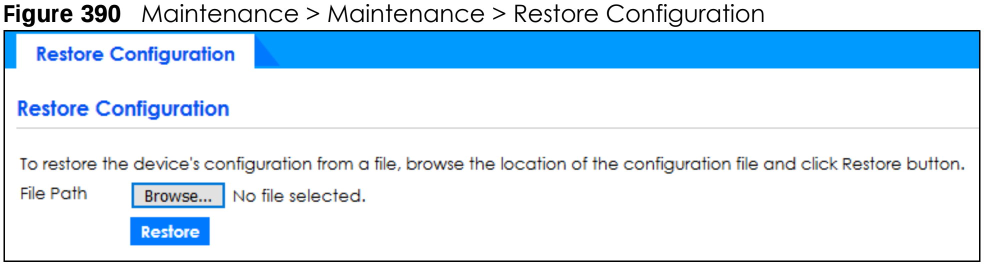
Click **Custom Default** and follow steps 1 to 2 to reboot and load a customized default file on the Switch.

64.5 Restore Configuration

You can restore a previously saved device configuration from your computer.

Click **Maintenance** > **Maintenance** > **Restore Configuration** to display the screen as shown next. Use this screen to restore a previously saved configuration from your computer.

Figure 390 Maintenance > Maintenance > Restore Configuration

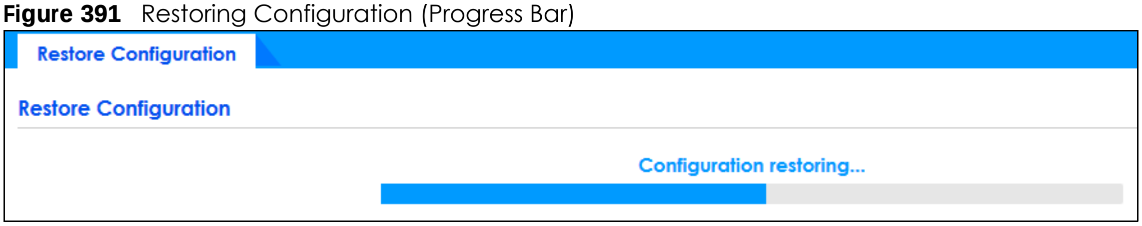


Follow the steps below to restore a previously saved configuration from your computer in this screen.

1 Click **Choose File** or **Browse** to locate the configuration file you wish to restore to the Switch.

2 Click **Restore**. The restore progress is shown.

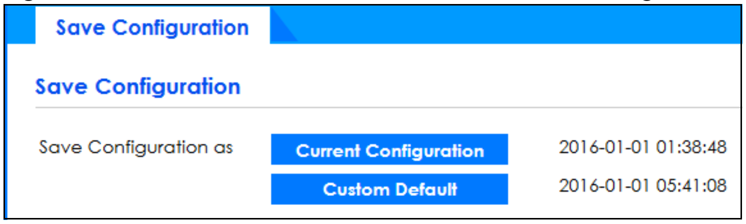
Figure 391 Restoring Configuration (Progress Bar)



64.6 Save Configuration

Click **Maintenance** > **Maintenance** > **Save Configuration** to view the screen as shown next.

Figure 392 Maintenance > Maintenance > Save Configuration



Click **Current Configuration** to save the current configuration settings permanently to the Switch. This configuration is set up according to your network environment.

Click **Custom Default** to save the current configuration settings permanently to a customized default file on the Switch.

Note: If a customized default file was not saved, clicking **Custom Default** in the **Maintenance** > **Reboot System** screen loads the factory default configuration on the Switch.

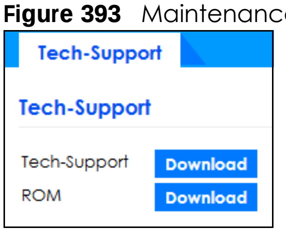
Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

64.7 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 **Maintenance** > **Maintenance** > **Tech-Support** to see the following screen.

Figure 393 Maintenance > 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 276 Maintenance > Maintenance > Tech-Support

LABEL	DESCRIPTION
Tech-Support	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.
ROM	Click **Download** to see the Read Only Memory (ROM) log report. This report is stored in flash memory.

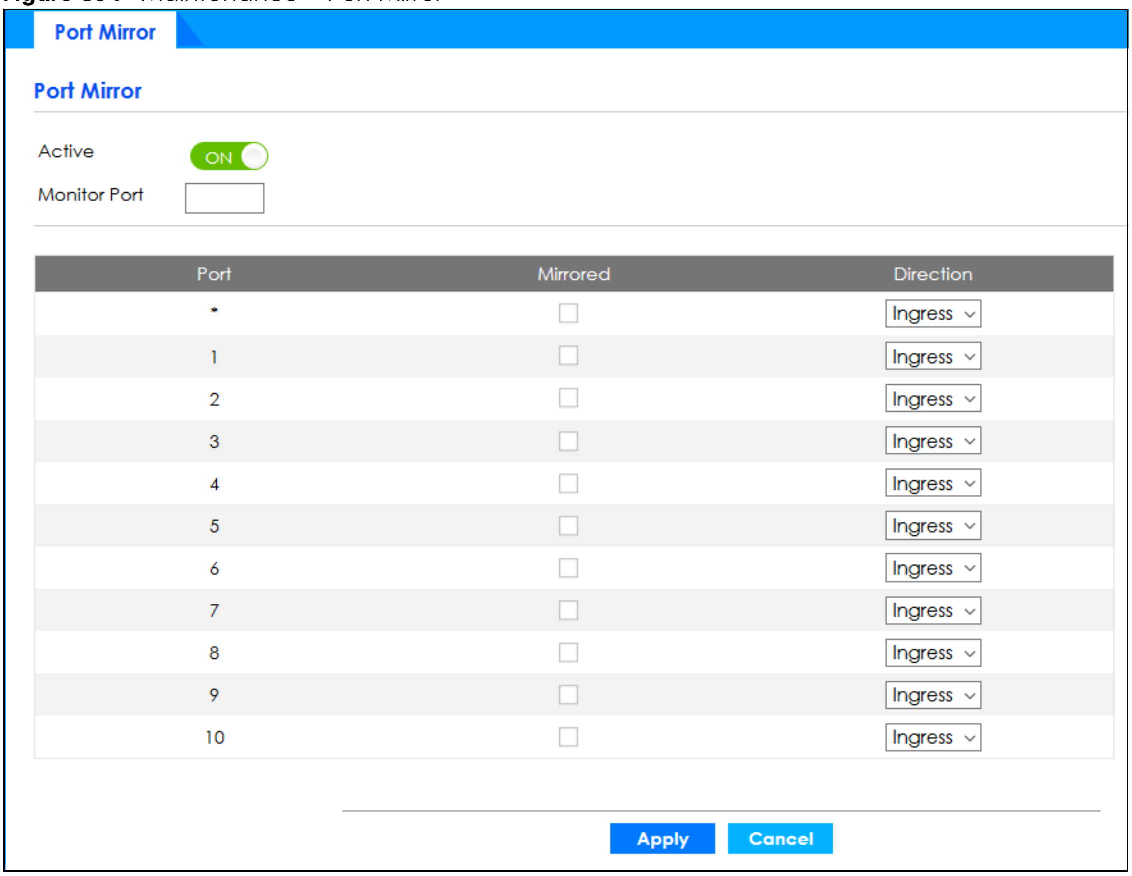
64.8 Port Mirroring

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.

Use the **Port Mirror** screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Click **Maintenance** > **Port Mirror** in the navigation panel to display the **Port Mirror** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 394 Maintenance > Port Mirror



The following table describes the labels in this screen.

Table 277 Maintenance > Port Mirror

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 ports. Enter the port number of the monitor port.
Port	This field displays the port number.

Table 277 Maintenance > Port Mirror (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 non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

PART III
Troubleshooting and Appendices

CHAPTER 65
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

65.1 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.

2 Make sure you are using the power adapter or cord included with the Switch.

3 Make sure the power adapter 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.

5 Disconnect and re-connect the power adapter or cord to the Switch.

6 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 47.

2 Check the hardware connections. See Section 3.1 on page 39.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the Switch off and on.

5 Disconnect and re-connect the power adapter or cord to the Switch.

6 If the problem continues, contact the vendor.

65.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default in-band IP address in standalone mode is **http://DHCP-assigned IP** (when connecting to a DHCP server) or **192.168.1.1**.

2 Use the ZON utility to find the IP address.

3 If this does not work, you have to reset the device to its factory defaults. See Section 4.8 on page 76.

I forgot the user name and/or password.

1 The default user name 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 4.8 on page 76.

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 in standalone mode is http://DHCP-assigned IP (when connecting to a DHCP server) or 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 47.

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 4.8 on page 76.

6 If the problem continues, contact the vendor, or try the advanced suggestion.

Advanced Suggestion

- 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 sessions 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 4.8 on page 76.

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).

There is unauthorized access to my Switch via telnet, HTTP and SSH.

To avoid unauthorized access, configure the secured client setting in the **Management** > **Access Control** > **Remote Management** screen for telnet, HTTP and SSH (see Section 47.6 on page 415). Computers not belonging to the secured client set cannot get permission to access the Switch.

65.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's non-volatile 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 46.2.2 on page 394 for more information about how to save your configuration.

I accidentally unplugged the Switch. I am not sure which configuration file will be loaded.

If you plug the power cable back to the Switch, it will reboot and load the configuration file that was used the last time. For example, if **Config 1** was used on the Switch before you accidentally unplugged the Switch, **Config 1** will be loaded when rebooting.

APPENDIX A
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 *https://www.zyxel.com/homepage.shtml* and also *https://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.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd.
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://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
- https://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd.
- https://www.zyxel.com/th/th/

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

Europe

Belarus

- Zyxel BY
- https://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/

- https://www.zyxel.com/be/fr/

Bulgaria

- Zyxel България
- https://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

Estonia

- Zyxel Estonia
- https://www.zyxel.com/ee/et/

Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

France

- Zyxel France
- https://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

Italy

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

Latvia

- Zyxel Latvia
- https://www.zyxel.com/lv/lv/

Lithuania

- Zyxel Lithuania
- https://www.zyxel.com/lt/lt/

Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

Romania

- Zyxel Romania
- https://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd.
- https://www.zyxel.com/es/es/

Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

Middle East

- Zyxel Communications Corporation
- https://www.zyxel.com/me/en/

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- https://www.zyxel.com/us/en/

Oceania

Australia

- Zyxel Communications Corporation
- https://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- https://www.zyxel.com/za/en/

Appendix B 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 278 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 email.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client or server protocol for the world wide web.

Table 278 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 or 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 email 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 278 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.

APPENDIX C
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 279 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 280 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 cannot be assigned to a multicast group.

Table 281 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
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 4 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 282

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

Table 283

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

Stateless Auto-configuration

With stateless auto-configuration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version 6) which is used in IPv6 stateful auto-configuration, the owner and status of addresses do not 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 [3]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

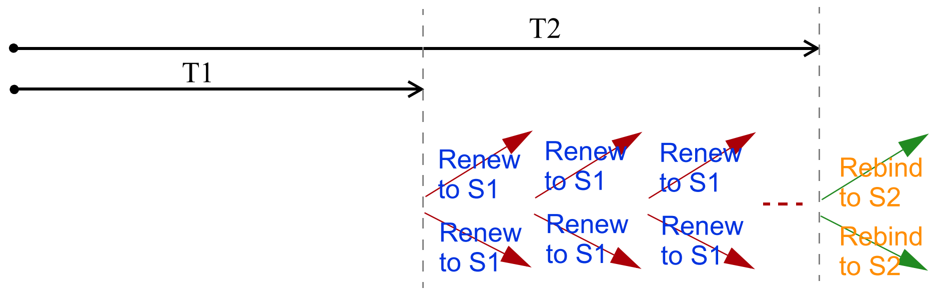
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

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

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, 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 or 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.)

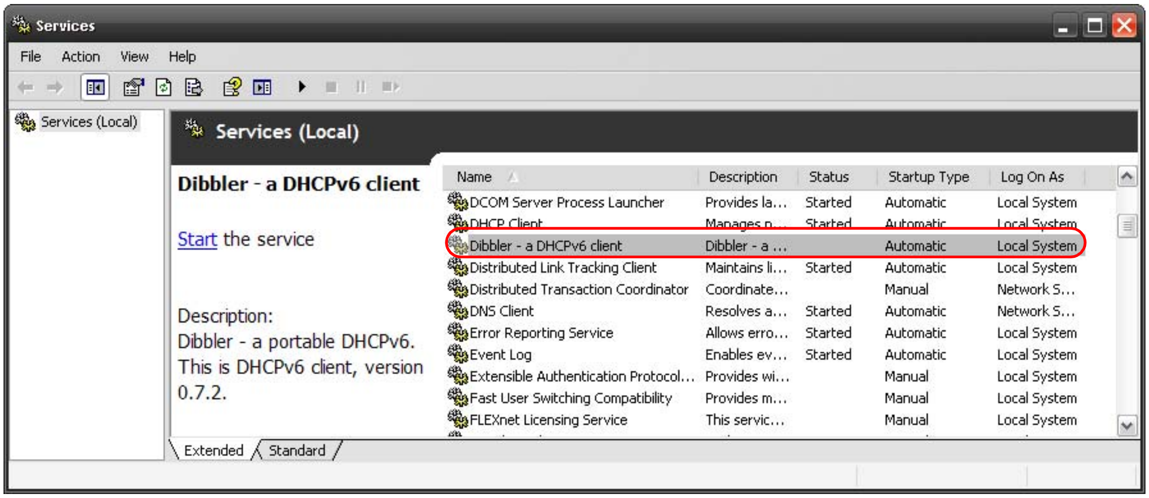
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

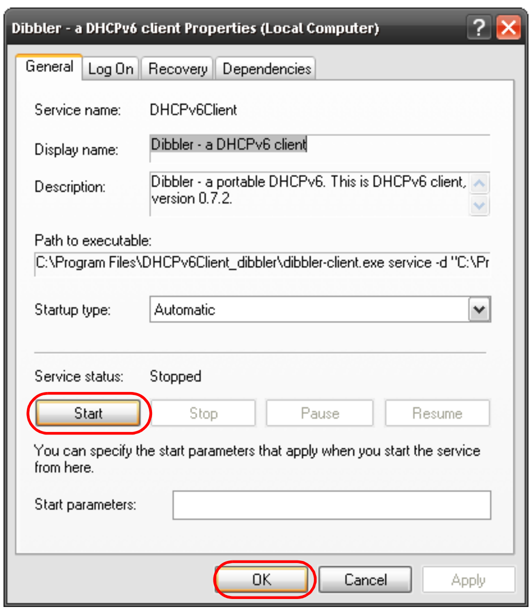
2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

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

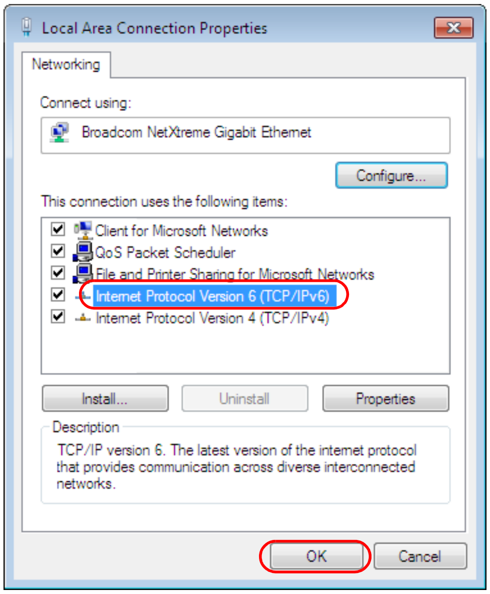
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

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)** check box 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
```

APPENDIX D
Legal Information

Copyright

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.

Innovation, Science and Economic Development 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

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

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

- To avoid possible eye injury, do NOT look into an operating fiber-optic module's connector.
- 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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- 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.
- Please use the provided or designated connection cables/power cables/adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. 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 IS REPLACED BY AN INCORRECT TYPE, DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTION. Dispose them at the applicable collection point for the recycling of electrical and electronic device. 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.
- 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.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  – For PERMANENTLY CONNECTED DEVICES, a readily accessible disconnect device shall be incorporated external to the device;

  – For PLUGGABLE DEVICES, the socket-outlet shall be installed near the device and shall be easily accessible.
- This device must be grounded by qualified service personnel. Never defeat the ground conductor or operate the device 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.

- CLASS 1 LASER PRODUCT (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

- APPAREIL À LASER DE CLASS 1 (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

Important Safety Instructions

1. Warning! Energy Hazard. Remove all metal jewelry, watches, and so on from your hands and wrists before serving this device.
2. Caution! The RJ-45 jacks are not used for telephone line connection.
3. Hazardous Moving Parts. Keep body parts away from fan blades.
4. Hot Surface. Do not touch.

1. Avertissement: Risque de choc électrique. Retirer tout bijoux en métal et votre montre de vos mains et poignets avant de manipuler cet appareil.
2. Attention: Les câbles RJ-45 ne doivent pas être utilisés pour les connections téléphoniques.
3. Mobilité des pièces détachées. S'assurer que les pièces détachées ne sont pas en contact avec les pales du ventilateur.
4. Surface brûlante. Ne pas toucher.

Environment Statement

European Union - Disposal and Recycling Information

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.

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。」

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。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

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 at www.zyxel.com to receive email notices of firmware upgrades and related information.

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.

Index

Numerics

802.1P priority 113, 475

A

AAA 248
- accounting 248
- authentication 248
- authorization 248
- external server 248
- RADIUS 248

AAA (Authentication, Authorization and Accounting) 248

Access Control
- overview 406, 501

access control
- limitations 406, 501
- login account 412, 501
- remote management 415, 503
- service port 414, 510
- SNMP 416

Access Control screen 406

accounting
- setup 253

add or edit static VLAN 487

add or edit VLAN 495, 497

Address Resolution Protocol (ARP) 388, 446, 449, 451

administrator password 53, 413, 502

AES (Advanced Encryption Standard) 510

age 171

aging time 105

All connected
- Setting Wizard 153

anti-arpscan 344
- blocked hosts 345
- host threshold 347
- status 345
- trusted hosts 346

applications
- backbone 28
- bridging 29
- fiber uplink 29
- IEEE 802.1Q VLAN 30
- PoE 28
- switched workgroup 30

ARP
- how it works 388
- learning mode 388
- overview 388
- setup 390

ARP (Address Resolution Protocol) 446

ARP inspection 260, 290
- and MAC filter 290
- configuring 291
- syslog messages 291
- trusted ports 290

ARP Learning screen 390

ARP scan 344

ARP Setup screen 390

ARP Table screen 446

ARP-Reply 388

ARP-Request 389

authentication
- setup 253

authentication, authorization and accounting 248

authorization
- privilege levels 255
- setup 253

auto PD recovery 363
- enable 363
- restart 363
- use LLDP or ping 363

auto-crossover port 41

automatic PD recovery
- create 365

automatic VLAN registration 134, 483

auto-MDIX port 41

B

back up
configuration file 398, 512
Backup Configuration screen 398, 512, 515
bandwidth control 183, 184
egress rate 184
ingress rate 184
setup 183
Bandwidth Control screen 183
basic settings 100
basic setup tutorial 83
Basic TLV Setting screen 337
binding table 260
building 260, 266
BPDU 349
BPDU (Bridge Protocol Data Units) 349
BPDU guard 349
and Errdisable Recovery 349
port status 349
BPDUs 163
Bridge Protocol Data Units 349
Bridge Protocol Data Units (BPDUs) 163
broadcast storm control 185
Broadcast Storm Control screen 476

C

CDP 301
CE EMC statement 541
Certificates screen 401
certifications
viewing 545
CFI (Canonical Format Indicator) 134, 483
changing the password 74
Cisco Discovery Protocol, see CDP
CIST 182
Class of Service 371
classifier 209
and QoS 209
editing 214
example 216
logging 215
match order 215
overview 209
setup 210, 214
status 210
viewing 214
cloning a port, see port cloning
Cloud Management screen 468
cluster management 437
and switch passwords 440
cluster manager 437, 440
cluster member 437, 440
cluster member firmware upgrade 441
network example 437
setup 439
specification 437
status 438
switch models 437
VID 440
Web Configurator 441
Cluster Management Configuration screen 439
cluster manager 437
Common and Internal Spanning Tree, see CIST 182
configuration 368
change running config 394, 514
save 516
saving 75
configuration file
backup 398, 512
restore 397, 515
save 394, 516
Configure Clone screen 449
console port
settings 44
contact information
customer support 524
copying port settings, see port cloning
copyright 541
CoS 371
CPU management port 151
CPU protection 311
current date 103, 467
current time 103, 466
custom default
restore 76
customer support 524

D

date
current 103
daylight saving time 104, 467
DDMI Details screen 459
DDMI screen 458
DES (Data Encryption Standard) 510
DHCP
configuration options 376
Dynamic Host Configuration Protocol 375
modes 375
Relay Agent Information format 377
setup 376
DHCP Option 82 Profile screen 378
DHCP relay
configure 90
tutorial 87
DHCP relay agent 536
DHCP relay option 82 275
DHCP Relay screen 380, 382
DHCP screen 376
DHCP snooping 83, 260, 274
configure 275
DHCP relay option 82 275
trusted ports 274
untrusted ports 274
DHCP snooping database 274
DHCP Snooping Port Configure screen 85
DHCP Status screen 376
DHCP Unique IDentifier (DUID) 536
DHCP-assigned IP 521
DHCPv4
global relay 379
global relay example 381
Option 82 377
option 82 profiles 378
Relay Agent Information 377
DHCPv4 relay 377
DHCPv6
enable in Windows XP 538
DHCPv6 Client Setup screen 130
DHCPv6 relay 385
interface-ID 385
remote-ID 385
DHCPv6 Relay screen 386
diagnostics 430
Ethernet port test 431
ping 431
Differentiated Service (DiffServ) 371
DiffServ 371
activate 372
DS field 371
DSCP 371
network example 372
PHB 371
service level 371
DiffServ Code Points 371
Digital Diagnostics Monitoring Interface 458
disclaimer 541
disposal and recycling information
EU 543
DS (Differentiated Services) 371
DSCP 371
what it does 371
dual firmware images 396, 513
Dynamic Host Configuration Protocol for IPv6 (DHCPv6) 535
dynamic link aggregation 189

E

egress port 153
egress rate 184
electrostatic discharge (ESD) 41
Environment Statement 543
Errdisable Detect screen 315
Errdisable Recovery screen 316
Errdisable screen 312
errdisable status 314
error disable 311
control packets 313
CPU protection 314
detect 315
recovery 316
status 312
error-disable recovery 311
Ethernet broadcast address 388, 446
Ethernet MAC 101, 465
Ethernet OAM 352

Ethernet port
- auto-crossover **40**
- auto-negotiating **40**
- dual personality **41**

Ethernet port test **431**

Ethernet settings
- default **41**

external authentication server **249**

F

FCC interference statement **541**

fiber optic cable
- connecting **42**
- removal **43**

file transfer using FTP
- command example **404**

filename convention, configuration
- file names **403**

filtering **160**
- rules **160**

filtering database, MAC table **443**

Filtering screen **160**

firmware **465**
- upgrade **396**, **441**, **513**
- ZyNOS **101**

firmware upgrade **513**

Firmware Upgrade screen **396**

flow control
- back pressure **113**, **475**
- IEEE802.3x **113**, **475**

forwarding
- delay **171**, **172**

frames
- tagged **142**, **489**
- untagged **142**, **489**

front panel **39**

FTP **403**
- file transfer procedure **404**
- restrictions over WAN **405**

G

GARP (Generic Attribute Registration Protocol) **134**, **483**

GARP timer **105**, **135**, **483**

general setup **102**

General Setup screen **102**, **465**

getting help **77**

gigabit ports **40**

GMT (Greenwich Mean Time) **104**, **467**

gratuitous ARP **389**

green Ethernet **320**
- and uplink port **320**
- auto power down **320**
- EEE **320**
- short reach **320**

grounding **45**

GVRP **135**, **484**

GVRP (GARP VLAN Registration Protocol) **135**, **484**

H

hardware installation **33**

hardware monitor **101**, **465**

hardware overview **39**

Hello Time **172**

hello time **170**

hops **171**

HTTPS **424**
- certificates **424**
- implementation **424**
- public keys, private keys **424**

HTTPS Certificates screen **402**

HTTPS example **424**

I

IANA (Internet Assigned Number Authority) **530**

Identity Association (IA) **536**

IEEE 802.1x
- activate **198**
- port authentication **196**
- reauthentication **199**

IEEE 802.3af **27**
IEEE 802.3at **27**
IEEE 802.3az **320**
IGMP
  overview **371**
IGMP filtering
  profile **234**, **496**
IGMP leave timeout
  fast **232**, **493**
  normal **232**, **493**
IGMP snooping **226**
  MVR **227**
IGMP snooping and VLANs **226**
IGMP throttling **232**, **493**
ingress port **153**
ingress rate **184**
initial setup **78**
Innovation, Science and Economic Development Canada ICES statement **541**
installation
  air circulation **33**
  desktop **33**
  rack-mounting **36**
  transceiver **42**
  wall mounting **34**
installation requirements
  wall mounting **34**
installation scenarios **33**
Interface Setup screen **119**
Internet Protocol version 6, see IPv6
IP
  configuration **108**
  status **107**
IP address **107**, **108**
IP setup **499**
IP Setup screen **82**, **106**, **499**
IP source guard **260**
  ARP inspection **260**, **290**
  DHCP snooping **260**
  static bindings **260**
IP Status Detail screen **107**
IP subnet mask **107**, **108**
IPv4 Multicast
  status **490**
IPv4 Multicast Status screen **490**
IPv6 **31**, **533**
  addressing **533**
  enable in Windows 7 **539**
  EUI-64 **535**
  global address **533**
  interface ID **535**
  link-local address **533**
  Neighbor Discovery Protocol **31**, **533**
  neighbor table **452**
  ping **31**, **533**
  prefix **533**
  prefix length **533**
  stateless auto-configuration **535**
  unspecified address **534**
IPv6 cache **537**
IPv6 Configuration screen **123**
IPv6 Global Address Setup screen **126**
IPv6 Global Setup screen **123**
IPv6 interface **119**
  DHCPv6 client **129**
  enable **124**
  global address **126**
  global unicast address **122**
  link-local address **125**
  link-local IP **122**
  neighbor discovery **127**
  neighbor table **128**
  stateless auto-configuration **124**
  status **120**
IPv6 Interface Setup screen **125**
IPv6 Interface Status screen **121**
IPv6 Link-Local Address Setup screen **125**
IPv6 multicast
  status **236**
IPv6 Neighbor Setup screen **129**
IPv6 neighbor table **452**
IPv6 Neighbor Table screen **452**
IPv6 screen **120**

J

Java permission **50**, **522**
JavaScript **50**, **522**

L

L2PT 299
- access port 300
- CDP 299
- configuration 300
- encapsulation 299
- example 300
- LACP 300
- MAC address 299, 301
- mode 300
- overview 299
- PAgP 300
- point to point 300
- STP 299
- tunnel port 300
- UDLD 300
- VTP 299

LACP 189, 302
- system priority 193, 481
- timeout 194, 482

Layer 2 protocol tunneling, see L2PT

LED description 47

LEDs 47

limit MAC address learning 206

link aggregation 63, 189
- dynamic 189
- ID information 190
- setup 191, 478
- traffic distribution algorithm 191, 478
- traffic distribution type 192, 480
- trunk group 189

Link aggregation (trunking) 478

Link Aggregation Control Protocol (LACP) 189

Link Aggregation Control Protocol screen 480

Link Aggregation Setting screen 478

Link Aggregation Status screen 477

Link Layer Discovery Protocol 322

LLDP 322
- basic TLV 337
- global settings 336
- local port status 326
- organization-specific TLV 338
- status of remote device 330
- TLV 322

LLDP (Link Layer Discovery Protocol) 322

LLDP screen 324

LLDP-MED 323
- classes of endpoint devices 323
- example 323

LLDP-MED Configuration screen 339

LLDP-MED Location screen 341

lockout 75
- Switch 75

log message 433

login 50
- password 74
- privilege level 414

login account
- administrator 412, 501
- non-administrator 412, 501

login accounts 412, 501
- configuring via Web Configurator 412, 501
- multiple 412, 501
- number of 412, 501

login password 502
- edit 413

Logins screen 412, 501

loop guard 292
- examples 293
- port shut down 293
- setup 294
- vs. STP 292

M

MAC (Media Access Control) 101, 465

MAC address 101, 446, 465
- maximum number per port 206

MAC address learning 105, 206
- specify limit 206

MAC Based VLAN screen 149

MAC filter
- and ARP inspection 290

MAC freeze 206

MAC table 443
- display criteria 445
- how it works 443
- sorting criteria 445
- transfer type 445
- viewing 444

MAC-based VLAN 148

maintenance 392
  configuration backup 398, 512
  current configuration 393
  firmware 396, 513
  main screen 393
  restore configuration 397, 515
Maintenance screen 392
Management Information Base (MIB) 417, 505
management IP address 81
management port 153
managing the device
  cluster management 32
  good habits 32
  NCC 31
  using FTP, see FTP 31
  using SNMP 31
  using Telnet, see command interface 31
  using the command interface, see command interface 31
  ZON Utility 32
man-in-the-middle attacks 290
max
  age 171
  hops 171
maximum transmission unit 448
Maximum Transmission Unit (MTU) 121
Mbuf (Memory Buffer) 400, 516
MD5 (Message Digest 5) 510
MDIX (Media Dependent Interface Crossover) 41
Media Access Control 101, 465
Memory Buffer 400
MIB
  and SNMP 417, 505
  supported MIBs 417
MIB (Management Information Base) 417, 505
mirroring ports 187, 517
MLD filtering profile 241
MLD snooping-proxy 236
  filtering 240
  filtering profile 241
  port role 238
  VLAN ID 237
monitor port 187, 517
mounting brackets 37
MST Instance, see MSTI 182
MST region 181
MSTI 173, 182
MSTI (Multiple Spanning Tree Instance) 173
MSTP 164
  bridge ID 175
  configuration 169
  configuration digest 176
  forwarding delay 171, 172
  Hello Time 172, 175
  hello time 170
  Max Age 172, 175
  max age 171
  max hops 171
  maximum hops 172
  path cost 172
  port priority 171
  revision level 171, 172
  status 174
MTU 448
MTU (Multi-Tenant Unit) 104
multicast
  IGMP throttling 232, 493
  IP addresses 225
  setup 229
multicast group 234, 496
multicast MAC address 156
Multiple Spanning Tree Protocol, see MSTP 164
Multiple STP 164
Multi-Tenant Unit 104
MVR 227
  configuration 242
  network example 227
MVR (Multicast VLAN Registration) 227

N

navigation panel
  Standard mode 70
  Surveillance mode 73
Nebula Switch Registration screen 132
Neighbor Detail screen 98
Neighbor Discovery Protocol (NDP) 537
Neighbor screen 96
network applications 27
network element (NE) 504
network management system (NMS) 416, 504

Networked AV mode **27**, **461**
overview **461**
Networked AV screen
Wizard **61**, **66**
NTP (RFC-1305) **103**, **466**

O

OAM **352**
details **353**
discovery **352**
port configuration **352**
remote loopback **352**, **357**
one-time schedule **207**
Operations, Administration and Maintenance **352**
Option 82 **377**
Organizationally Unique Identifiers (OUI) **147**
Org-specific TLV Setting screen **338**

P

PAGP **302**
password **74**
administrator **53**, **413**, **502**
change via Wizard **60**, **65**
password change
via Password / SNMP link **52**
Path MTU Discovery **448**
Path MTU Table screen **448**
Per-Hop Behavior **371**
PHB **371**
ping, test connection **431**
PoE
PD priority **117**, **472**
power management mode **117**, **472**
power-up mode **116**, **469**, **471**
PoE (Power over Ethernet) **113**
PoE features
by model **27**
PoE Setup screen **116**
PoE standards **27**
PoE Status screen **114**
PoE Time Range Setup screen **116**
policy **219**
and classifier **219**
and DiffServ **218**
configuration **219**
example **221**
overview **218**
rules **218**, **219**
port
setup **111**
speed/duplex **112**
Port Aggregation Protocol, see PAgP
port authentication **196**
guest VLAN **201**
IEEE802.1x **198**
MAC authentication **199**
method **198**
Port Based VLAN Setup screen **152**
port cloning **449**, **451**
advanced settings **449**, **451**
basic settings **449**, **451**
port details **455**
Port isolation
Setting Wizard **153**
Port Mirror screen **517**
port mirroring **187**, **517**
port redundancy **189**
Port screen
DHCPv4 Global Relay **380**
DHCPv4 VLAN **383**
SNMP traps **507**
port security **205**
address learning **206**
limit MAC address learning **206**
setup **205**
port setup **473**
Port Setup screen **111**, **473**
port status **454**
port details **455**
port utilization **460**
port utilization **460**
Port VID (PVID) **80**
port VLAN ID, see PVID **142**, **489**
port VLAN trunking **135**, **484**
port-based VLAN **151**
all connected **153**
configure **151**
port isolation **153**

settings wizard **153**
ports
diagnostics **431**, **432**
mirroring **187**, **517**
speed/duplex **474**
standby **190**
power
voltage **102**
power connections **46**
power connector **46**
power status **102**
powered device (PD) **113**
PPPoE IA **303**
agent sub-options **305**
configuration **305**
drop PPPoE packets **307**
port state **305**
sub-option format **304**
tag format **304**
trusted ports **305**
untrusted ports **305**
VLAN **309**
PPPoE Intermediate Agent **303**
prefix delegation **536**
priority level
queue assignment **106**
priority queue assignment **106**
priority, and OSPF **370**
product registration **545**
PVID **134**, **483**

Q

QoS **371**
and classifier **209**
Quality of Service **371**
queue weight **223**
queuing **222**, **223**
SPQ **222**
WRR **222**
queuing method **222**, **224**

R

rack-mounting **36**
installation requirements **36**
precautions **37**
RADIUS **249**
advantages **249**
setup **249**
Rapid Spanning Tree Protocol (RSTP) **162**
Read Only Memory (ROM) **516**
rear panel **44**
reboot
load configuration **394**, **514**
reboot system **394**, **514**
Reboot System screen **514**
recurring schedule **207**
registration
product **545**
Regulatory Notice and Statement **541**
remote management **415**, **503**
service **416**, **504**
trusted computers **416**, **504**
Remote Management screen **503**
RESET button **76**
resetting **76**, **394**, **395**
to custom default settings **395**
to factory default settings **394**, **395**
restore
configuration file **515**
RESTORE button **76**
restore configuration **397**
restoring configuration **76**
RFC 3164 **434**
Round Robin Scheduling **222**
Router Advertisement (RA) **536**
RSTP
configuration **168**
rubber feet
attach **34**
running configuration **394**
erase **394**
reset **394**

S

safety warnings **542**
save configuration **75**, **394**, **516**
Save Configuration screen **515**
Save link **75**
schedule
  one-time **207**
  recurring **207**
  type **208**
screw anchors
  using **35**
Secure Shell, see SSH
service access control **414**, **510**
  service port **414**, **511**
Service Access Control screen **511**
Setup Wizard
  parts **58**
Setup Wizard screen **52**
sFlow
  collector **303**
SHA (Secure Hash Algorithm) **510**
Simple Network Management Protocol (SNMP) **504**
Simple Network Management Protocol, see SNMP
Small Form-factor Pluggable (SFP) **41**
SNMP **416**
  agent **416**, **504**
  and MIB **417**, **505**
  authentication **411**, **412**, **509**, **510**
  communities **53**, **408**, **506**
  management model **416**, **504**
  manager **417**, **504**
  MIB **417**
  network components **416**, **504**
  object variables **417**, **504**
  protocol operations **417**, **505**
  security **411**, **509**, **510**
  security level **412**
  settings **504**
  setup **407**, **504**
  traps **408**, **506**
  users **410**, **509**
  version 3 and security **417**, **505**
  versions supported **416**, **504**
SNMP agent
  enable via Wizard **60**, **65**
SNMP screen **505**
SNMP traps **417**
  supported **418**, **419**, **421**
SNMP version
  select **60**, **65**
SPQ (Strict Priority Queuing) **222**
SSH
  encryption methods **423**
  how it works **422**
  implementation **423**
SSH (Secure Shell) **422**
SSL (Secure Socket Layer) **424**
standby ports **190**
static bindings **260**
static MAC address **154**
static MAC forwarding **154**
Static MAC Forwarding screen **154**
static multicast forwarding **156**
Static Multicast Forwarding screen **157**
static route **368**
  enable **370**
  metric **370**
  overview **368**
static VLAN **139**, **486**
  control **140**, **488**
  tagging **140**, **488**
Static VLAN screen **79**, **486**
status **68**, **94**, **461**
  IPv4 Multicast **490**
  MSTP **174**
  port **454**
  power **102**
  STP **166**
  VLAN **137**, **485**
Status screen **94**
STP **301**
  bridge ID **167**, **179**
  bridge priority **168**, **178**
  designated bridge **163**
  edge port **169**, **178**
  forwarding delay **169**
  Hello BPDU **163**
  Hello Time **167**, **168**, **178**, **179**
  how it works **163**
  Max Age **167**, **168**, **178**, **179**
  path cost **163**, **169**, **178**
  port priority **169**, **178**
  port role **167**, **180**

port state **163**, **167**, **180**
root port **163**
status **165**, **166**
terminology **163**
vs. loop guard **292**
STP Path Cost **163**
subnet based VLANs **142**
subnet masking **535**
Summary screen **461**
Switch
DHCP client **50**
switch lockout **75**
Switch reset **76**
Switch Setup screen **105**
syslog **291**, **434**
protocol **434**
settings **434**
setup **434**
severity levels **434**
Syslog Setup screen **434**
System Info screen **100**, **464**
system reboot **394**, **514**

T

TACACS+ **249**
advantages **249**
setup **251**
tagged VLAN **134**, **483**
Tech-Support **399**, **516**
log enhancement **399**, **516**
Tech-Support screen **399**
temperature indicator **102**, **465**
terminal emulation software
parameters **44**
time
current **103**, **466**
daylight saving **104**
format **103**
Time (RFC-868) **103**, **466**
time range **207**
time server **103**, **466**
time service protocol **103**, **466**
format **466**
ToS **371**
trademarks **545**
transceiver
connection speed **41**
installation **42**
removal **42**
transceiver MultiSource Agreement (MSA) **41**
transceivers **41**
Trap Group screen **408**, **506**
traps
destination **408**, **506**
troubleshooting **91**
trunk group **189**
trunking **189**
trusted ports
ARP inspection **290**
DHCP snooping **274**
PPPoE IA **305**
tutorial
DHCP snooping **83**
tutorials **83**
Type of Service **371**

U

UDLD **302**
UniDirectional Link Detection, see UDLD
untrusted ports
ARP inspection **290**
DHCP snooping **274**
PPPoE IA **305**
User Information screen
SNMP **410**, **509**
user name **51**
default **51**
user profiles **249**
UTC (Universal Time Coordinated) **104**

V

Vendor ID Based VLAN screen **150**
Vendor Specific Attribute, see VSA **255**
VID **110**, **137**, **138**, **485**, **486**, **500**

number of possible VIDs **134**, **483**
priority frame **134**, **483**
VID (VLAN Identifier) **134**, **483**
View-based Access Control Model (VACM) **510**
Virtual Local Area Network **104**
VLAN **104**
acceptable frame type **142**, **489**
and IGMP snooping **226**
automatic registration **134**, **483**
creation **87**
ID **134**, **483**
ingress filtering **142**, **489**
introduction **104**, **134**, **483**
number of VLANs **137**, **485**
port number **138**, **486**
port settings **141**, **488**
port-based **153**
port-based VLAN **151**
port-based, isolation **153**
port-based, wizard **153**
PVID **142**, **489**
static VLAN **139**, **486**
status **137**, **138**, **485**, **486**
subnet based **142**
tagged **134**, **483**
terminology **135**, **484**
trunking **135**, **142**, **484**, **489**
type **105**, **136**
VLAN (Virtual Local Area Network) **104**
VLAN Detail screen **485**
VLAN ID **134**, **483**
VLAN mapping **295**
activating **296**
configuration **296**
example **295**
priority level **295**
tagged **295**
traffic flow **295**
untagged **295**
VLAN ID **295**
VLAN number **107**, **108**, **110**, **500**
VLAN Port Setting screen **488**
VLAN Setting screen **385**
DHCPv4 **382**
VLAN Status screen **485**
VLAN terminology **135**, **484**
VLAN trunking **142**, **489**
VLAN Trunking Protocol, see VTP
VLAN-unaware devices **79**
voice VLAN **147**
Voice VLAN Setup screen **147**
VSA **255**
VTP **301**

W

wall mounting **34**
distance above the floor **34**
distance between holes **34**
warranty **545**
note **545**
Web browser pop-up window **50**, **522**
Web Configurator
getting help **77**
home **68**
home screen **69**
login **50**
logout **76**
navigating components **69**
navigation panel **70**
online help **77**
usage prerequisite **50**
weight **223**
Windows OS version
check **54**
Wizard
link aggregation **63**
wizard
setup **68**
WRR (Weighted Round Robin Scheduling) **222**

Z

ZDP **54**
ZON (Zyxel One Network) **545**
ZON Utility **54**
compatible OS **54**
fields description **58**
icon description **57**
installation requirements **54**
introduction **27**

minimum hardware requirements 54
network adapter select 56
password prompt 57
run 55
supported firmware version 55
supported models 55
Switch IP address 50
ZON utility
use for troubleshooting 521
ZULD 359
example 359
probe time 361
status 360
ZULD (Zyxel Unidirectional Link Detection) 359
ZyNOS (Zyxel Network Operating System) 403, 545
Zyxel AP Configurator (ZAC) 58
Zyxel Discovery Protocol (ZDP) 54
Zyxel Unidirectional Link Detection 359
Zyxel Unidirectional Link Detection (ZULD) 359