

XGS-4526/4528F/4728F

Intelligent Layer 3+ Switch

User's Guide



Default Login Details

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

Firmware Version 4.00
Edition 1, 03/2011

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the Switch using the web configurator.

Related Documentation

- Web Configurator Online Help
The embedded Web Help contains descriptions of individual screens and supplementary information.
- Command Reference Guide
The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the Switch.

Note: It is recommended you use the web configurator to configure the Switch.

- Support Disc
Refer to the included CD for support documents.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- 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.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's 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

- The XGS-4526/4528F/4728F may be referred to as the “Switch”, the “device”, the “system” or the “product” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

The Switch 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- For continued protection against risk of fire replace only with same type and rating of fuse.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

User's Guide	25
Getting to Know Your Switch	27
Hardware Installation and Connection	33
Hardware Overview	37
The Web Configurator	47
Initial Setup Example	57
Tutorials	63
Technical Reference	93
System Status and Port Statistics	95
Basic Setting	101
VLAN	117
Static MAC Forward Setup	137
Static Multicast Forward Setup	141
Filtering	145
Spanning Tree Protocol	147
Bandwidth Control	169
Broadcast Storm Control	173
Mirroring	175
Link Aggregation	177
Port Authentication	187
Port Security	197
Classifier	201
Policy Rule	207
Queuing Method	215
VLAN Stacking	219
Multicast	227
AAA	243
IP Source Guard	259
Loop Guard	283
VLAN Mapping	287
Layer 2 Protocol Tunneling	291
sFlow	295
PPPoE	299
Error Disable	309
Private VLAN	315
Static Route	319
Policy Routing	323

RIP	327
OSPF	331
IGMP	345
DVMRP	349
Differentiated Services	353
DHCP	361
VRRP	371
ARP Learning	381
Load Sharing	387
Maintenance	389
Access Control	397
Diagnostic	423
Syslog	425
Cluster Management	435
MAC Table	443
IP Table	447
ARP Table	451
Routing Table	453
Configure Clone	455
Troubleshooting	457
Product Specifications	463

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
Contents Overview	9
Table of Contents.....	11
 Part I: User's Guide.....	 25
 Chapter 1	
Getting to Know Your Switch.....	27
1.1 Introduction	27
1.1.1 Bridging Example	27
1.1.2 High Performance Switching Example	28
1.1.3 Gigabit Ethernet to the Desktop	29
1.1.4 IEEE 802.1Q VLAN Application Example	29
1.1.5 IPv6 Support	30
1.2 Ways to Manage the Switch	30
1.3 Good Habits for Managing the Switch	31
 Chapter 2	
Hardware Installation and Connection	33
2.1 Freestanding Installation	33
2.2 Mounting the Switch on a Rack	34
2.2.1 Rack-mounted Installation Requirements	34
2.2.2 Attaching the Mounting Brackets to the Switch	34
2.2.3 Mounting the Switch on a Rack	35
 Chapter 3	
Hardware Overview.....	37
3.1 Front Panel Connections	37
3.1.1 Dual Personality Interfaces	38
3.1.2 1000Base-T Ports	38
3.1.3 Mini-GBIC Slots	39
3.2 Rear Panel	41

3.2.1 XGS-4526	41
3.2.2 XGS-4528F or XGS-4728F	41
3.2.3 Uplink Module	42
3.2.4 Rear Panel Connections	42
3.2.5 Power Connector	43
3.2.6 External Backup Power Supply Connector	44
3.2.7 Console Port	44
3.3 LEDs	45
Chapter 4	
The Web Configurator	47
4.1 Introduction	47
4.2 System Login	47
4.3 The Web Configurator Layout	48
4.3.1 Change Your Password	53
4.4 Saving Your Configuration	54
4.5 Switch Lockout	54
4.6 Resetting the Switch	54
4.6.1 Reload the Configuration File	55
4.7 Logging Out of the Web Configurator	56
4.8 Help	56
Chapter 5	
Initial Setup Example.....	57
5.1 Overview	57
5.1.1 Configuring an IP Interface	57
5.1.2 Configuring DHCP Server Settings	59
5.1.3 Creating a VLAN	59
5.1.4 Setting Port VID	61
5.1.5 Enabling RIP	62
Chapter 6	
Tutorials.....	63
6.1 How to Use DHCP Snooping on the Switch	63
6.2 How to Use DHCP Relay on the Switch	67
6.2.1 DHCP Relay Tutorial Introduction	67
6.2.2 Creating a VLAN	68
6.2.3 Configuring DHCP Relay	71
6.2.4 Troubleshooting	71
6.3 How to Use PPPoE IA on the Switch	72
6.3.1 Configuring Switch A	73
6.3.2 Configuring Switch B	75
6.4 How to Use Error Disable and Recovery on the Switch	77

6.5 How to Set Up a Guest VLAN	80
6.5.1 Creating a Guest VLAN	81
6.5.2 Enabling IEEE 802.1x Port Authentication	83
6.5.3 Enabling Guest VLAN	84
6.6 How to Do Port Isolation in a VLAN	85
6.6.1 Creating a VLAN	86
6.6.2 Creating a Private VLAN Rule	89
6.7 How to Configure Routing Policy	90
6.7.1 Create a Layer-3 Classifier	90
6.7.2 Create a Policy Routing Rule	91
 Part II: Technical Reference	 93
 Chapter 7	
System Status and Port Statistics	95
7.1 Overview	95
7.2 Port Status Summary	95
7.2.1 Status: Port Details	97
 Chapter 8	
Basic Setting	101
8.1 Overview	101
8.2 System Information	102
8.3 General Setup	104
8.4 Introduction to VLANs	106
8.4.1 Smart Isolation	107
8.5 Switch Setup Screen	108
8.6 IP Setup	110
8.6.1 IP Interfaces	110
8.7 Port Setup	113
 Chapter 9	
VLAN	117
9.1 Introduction to IEEE 802.1Q Tagged VLANs	117
9.1.1 Forwarding Tagged and Untagged Frames	117
9.2 Automatic VLAN Registration	118
9.2.1 GARP	118
9.2.2 GVRP	118
9.3 Port VLAN Trunking	119
9.4 Select the VLAN Type	120
9.5 Static VLAN	120

9.5.1 VLAN Status	121
9.5.2 VLAN Details	122
9.5.3 Configure a Static VLAN	122
9.5.4 Configure VLAN Port Settings	124
9.6 Subnet Based VLANs	126
9.7 Configuring Subnet Based VLAN	127
9.8 Protocol Based VLANs	128
9.9 Configuring Protocol Based VLAN	129
9.10 Create an IP-based VLAN Example	131
9.11 Port-based VLAN Setup	132
9.11.1 Configure a Port-based VLAN	132
Chapter 10	
Static MAC Forward Setup	137
10.1 Overview	137
10.2 Configuring Static MAC Forwarding	137
Chapter 11	
Static Multicast Forward Setup.....	141
11.1 Static Multicast Forwarding Overview	141
11.2 Configuring Static Multicast Forwarding	142
Chapter 12	
Filtering.....	145
12.1 Configure a Filtering Rule	145
Chapter 13	
Spanning Tree Protocol.....	147
13.1 STP/RSTP Overview	147
13.1.1 STP Terminology	147
13.1.2 How STP Works	148
13.1.3 STP Port States	149
13.1.4 Multiple RSTP	149
13.1.5 Multiple STP	150
13.2 Spanning Tree Protocol Status Screen	153
13.3 Spanning Tree Configuration	153
13.4 Configure Rapid Spanning Tree Protocol	154
13.5 Rapid Spanning Tree Protocol Status	156
13.6 Configure Multiple Rapid Spanning Tree Protocol	158
13.7 Multiple Rapid Spanning Tree Protocol Status	160
13.8 Configure Multiple Spanning Tree Protocol	162
13.8.1 Multiple Spanning Tree Protocol Port Configuration	165
13.9 Multiple Spanning Tree Protocol Status	166

Chapter 14	
Bandwidth Control	169
14.1 Bandwidth Control Overview	169
14.1.1 CIR and PIR	169
14.2 Bandwidth Control Setup	170
Chapter 15	
Broadcast Storm Control	173
15.1 Broadcast Storm Control Setup	173
Chapter 16	
Mirroring	175
16.1 Port Mirroring Setup	175
Chapter 17	
Link Aggregation	177
17.1 Link Aggregation Overview	177
17.2 Dynamic Link Aggregation	177
17.2.1 Link Aggregation ID	178
17.3 Link Aggregation Status	179
17.4 Link Aggregation Setting	181
17.5 Link Aggregation Control Protocol	183
17.6 Static Trunking Example	184
Chapter 18	
Port Authentication	187
18.1 Port Authentication Overview	187
18.1.1 IEEE 802.1x Authentication	187
18.1.2 MAC Authentication	188
18.2 Port Authentication Configuration	189
18.2.1 Activate IEEE 802.1x Security	190
18.2.2 Guest VLAN	191
18.2.3 Activate MAC Authentication	194
Chapter 19	
Port Security	197
19.1 About Port Security	197
19.2 Port Security Setup	198
19.3 VLAN MAC Address Limit	199
Chapter 20	
Classifier	201
20.1 About the Classifier and QoS	201

20.2 Configuring the Classifier	201
20.3 Viewing and Editing Classifier Configuration	204
20.4 Classifier Example	206
Chapter 21	
Policy Rule.....	207
21.1 Policy Rules Overview	207
21.1.1 DiffServ	207
21.1.2 DSCP and Per-Hop Behavior	207
21.2 Configuring Policy Rules	208
21.3 Viewing and Editing Policy Configuration	211
21.4 Policy Example	213
Chapter 22	
Queuing Method.....	215
22.1 Queuing Method Overview	215
22.1.1 Strictly Priority	215
22.1.2 Weighted Fair Queuing	215
22.1.3 Weighted Round Robin Scheduling (WRR)	216
22.2 Configuring Queuing	217
Chapter 23	
VLAN Stacking	219
23.1 VLAN Stacking Overview	219
23.1.1 VLAN Stacking Example	219
23.2 VLAN Stacking Port Roles	220
23.3 VLAN Tag Format	221
23.3.1 Frame Format	221
23.4 Configuring VLAN Stacking	222
23.4.1 Port-based Q-in-Q	223
23.4.2 Selective Q-in-Q	224
Chapter 24	
Multicast	227
24.1 Multicast Overview	227
24.1.1 IP Multicast Addresses	227
24.1.2 IGMP Filtering	227
24.1.3 IGMP Snooping	228
24.1.4 IGMP Snooping and VLANs	228
24.2 Multicast Status	228
24.3 Multicast Setting	229
24.4 IGMP Snooping VLAN	232
24.5 IGMP Filtering Profile	233

24.6 MVR Overview	235
24.6.1 Types of MVR Ports	235
24.6.2 MVR Modes	236
24.6.3 How MVR Works	236
24.7 General MVR Configuration	237
24.8 MVR Group Configuration	239
24.8.1 MVR Configuration Example	240
Chapter 25	
AAA	243
25.1 Authentication, Authorization and Accounting (AAA)	243
25.1.1 Local User Accounts	244
25.1.2 RADIUS and TACACS+	244
25.2 AAA Screens	244
25.2.1 RADIUS Server Setup	245
25.2.2 TACACS+ Server Setup	247
25.2.3 AAA Setup	249
25.2.4 Vendor Specific Attribute	252
25.2.5 Tunnel Protocol Attribute	253
25.3 Supported RADIUS Attributes	254
25.3.1 Attributes Used for Authentication	254
25.3.2 Attributes Used for Accounting	255
Chapter 26	
IP Source Guard.....	259
26.1 IP Source Guard Overview	259
26.1.1 DHCP Snooping Overview	260
26.1.2 ARP Inspection Overview	262
26.2 IP Source Guard	263
26.3 IP Source Guard Static Binding	264
26.4 DHCP Snooping	266
26.5 DHCP Snooping Configure	269
26.5.1 DHCP Snooping Port Configure	271
26.5.2 DHCP Snooping VLAN Configure	272
26.6 ARP Inspection Status	274
26.6.1 ARP Inspection VLAN Status	275
26.6.2 ARP Inspection Log Status	276
26.7 ARP Inspection Configure	277
26.7.1 ARP Inspection Port Configure	279
26.7.2 ARP Inspection VLAN Configure	280
Chapter 27	
Loop Guard.....	283

27.1 Loop Guard Overview	283
27.2 Loop Guard Setup	285
Chapter 28	
VLAN Mapping	287
28.1 VLAN Mapping Overview	287
28.1.1 VLAN Mapping Example	287
28.2 Enabling VLAN Mapping	288
28.3 Configuring VLAN Mapping	289
Chapter 29	
Layer 2 Protocol Tunneling.....	291
29.1 Layer 2 Protocol Tunneling Overview	291
29.1.1 Layer-2 Protocol Tunneling Mode	292
29.2 Configuring Layer 2 Protocol Tunneling	293
Chapter 30	
sFlow.....	295
30.1 sFlow Overview	295
30.2 sFlow Port Configuration	296
30.2.1 sFlow Collector Configuration	297
Chapter 31	
PPPoE	299
31.1 PPPoE Intermediate Agent Overview	299
31.1.1 PPPoE Intermediate Agent Tag Format	299
31.1.2 Sub-Option Format	300
31.1.3 Port State	301
31.2 The PPPoE Screen	302
31.3 PPPoE Intermediate Agent	302
31.3.1 PPPoE IA Per-Port	303
31.3.2 PPPoE IA Per-Port Per-VLAN	305
31.3.3 PPPoE IA for VLAN	307
Chapter 32	
Error Disable	309
32.1 CPU Protection Overview	309
32.2 Error-Disable Recovery Overview	309
32.3 The Error Disable Screen	310
32.4 CPU Protection Configuration	310
32.5 Error-Disable Detect Configuration	311
32.6 Error-Disable Recovery Configuration	313

Chapter 33	
Private VLAN	315
33.1 Private VLAN Overview	315
33.2 Configuring Private VLAN	316
Chapter 34	
Static Route	319
34.1 Static Routing Overview	319
34.2 Configuring Static Routing	320
Chapter 35	
Policy Routing	323
35.1 Policy Route Overview	323
35.1.1 Benefits	323
35.2 Configuring Policy Routing Profile	324
35.2.1 Policy Routing Rule Configuration	325
Chapter 36	
RIP	327
36.1 RIP Overview	327
36.1.1 Administrative Distance	327
36.2 Configuring RIP	328
Chapter 37	
OSPF	331
37.1 OSPF Overview	331
37.1.1 OSPF Autonomous Systems and Areas	331
37.1.2 How OSPF Works	332
37.1.3 Interfaces and Virtual Links	332
37.1.4 OSPF and Router Elections	333
37.1.5 Configuring OSPF	333
37.2 OSPF Status	334
37.3 OSPF Configuration	336
37.4 Configure OSPF Areas	337
37.4.1 View OSPF Area Information Table	339
37.5 Configuring OSPF Redistribution	339
37.6 Configuring OSPF Interfaces	341
37.7 OSPF Virtual-Links	343
Chapter 38	
IGMP	345
38.1 IGMP Overview	345
38.1.1 How IGMP Works	346

38.2 Port-based IGMP	347
38.3 Configuring IGMP	348
Chapter 39	
DVMRP	349
39.1 DVMRP Overview	349
39.2 How DVMRP Works	349
39.2.1 DVMRP Terminology	350
39.3 Configuring DVMRP	350
39.3.1 DVMRP Configuration Error Messages	351
39.4 Default DVMRP Timer Values	352
Chapter 40	
Differentiated Services	353
40.1 DiffServ Overview	353
40.1.1 DSCP and Per-Hop Behavior	353
40.1.2 DiffServ Network Example	354
40.2 Two Rate Three Color Marker Traffic Policing	354
40.2.1 TRTCM - Color-blind Mode	355
40.2.2 TRTCM - Color-aware Mode	355
40.3 Activating DiffServ	356
40.3.1 Configuring 2-Rate 3 Color Marker Settings	357
40.4 DSCP-to-IEEE 802.1p Priority Settings	359
40.4.1 Configuring DSCP Settings	360
Chapter 41	
DHCP	361
41.1 DHCP Overview	361
41.1.1 DHCP Modes	361
41.1.2 DHCP Configuration Options	361
41.2 DHCP Status	362
41.3 DHCP Server Status Detail	362
41.4 DHCP Relay	364
41.4.1 DHCP Relay Agent Information	364
41.4.2 Configuring DHCP Global Relay	365
41.4.3 Global DHCP Relay Configuration Example	366
41.5 Configuring DHCP VLAN Settings	367
41.5.1 Example: DHCP Relay for Two VLANs	369
Chapter 42	
VRRP	371
42.1 VRRP Overview	371
42.2 VRRP Status	372

42.3 VRRP Configuration	373
42.3.1 IP Interface Setup	373
42.3.2 VRRP Parameters	375
42.3.3 Configuring VRRP Parameters	376
42.3.4 Configuring VRRP Parameters	377
42.4 VRRP Configuration Examples	377
42.4.1 One Subnet Network Example	378
42.4.2 Two Subnets Example	379
Chapter 43	
ARP Learning	381
43.1 ARP Overview	381
43.1.1 How ARP Works	381
43.1.2 ARP Learning Mode	381
43.2 Configuring ARP Learning	384
Chapter 44	
Load Sharing	387
44.1 Load Sharing Overview	387
44.2 Configuring Load Sharing	387
Chapter 45	
Maintenance	389
45.1 The Maintenance Screen	389
45.2 Load Factory Default	390
45.3 Save Configuration	390
45.4 Reboot System	391
45.5 Firmware Upgrade	391
45.6 Restore a Configuration File	392
45.7 Backup a Configuration File	393
45.8 FTP Command Line	393
45.8.1 Filename Conventions	393
45.8.2 FTP Command Line Procedure	394
45.8.3 GUI-based FTP Clients	395
45.8.4 FTP Restrictions	395
Chapter 46	
Access Control	397
46.1 Access Control Overview	397
46.2 The Access Control Main Screen	397
46.3 About SNMP	398
46.3.1 SNMP v3 and Security	399
46.3.2 Supported MIBs	399

46.3.3 SNMP Traps	400
46.3.4 Configuring SNMP	407
46.3.5 Configuring SNMP Trap Group	409
46.3.6 Configuring SNMP User	410
46.4 Setting Up Login Accounts	412
46.5 SSH Overview	413
46.6 How SSH works	414
46.7 SSH Implementation on the Switch	415
46.7.1 Requirements for Using SSH	415
46.8 Introduction to HTTPS	415
46.9 HTTPS Example	416
46.9.1 Internet Explorer Warning Messages	416
46.9.2 Netscape Navigator Warning Messages	417
46.9.3 The Main Screen	419
46.10 Service Port Access Control	419
46.11 Remote Management	420
Chapter 47	
Diagnostic.....	423
47.1 Diagnostic	423
Chapter 48	
Syslog	425
48.1 Syslog Overview	425
48.2 Syslog Setup	426
48.3 Syslog Server Setup	427
48.4 Syslog Messages	428
Chapter 49	
Cluster Management.....	435
49.1 Clustering Management Status Overview	435
49.2 Cluster Management Status	436
49.2.1 Cluster Member Switch Management	437
49.3 Clustering Management Configuration	440
Chapter 50	
MAC Table.....	443
50.1 MAC Table Overview	443
50.2 Viewing the MAC Table	444
Chapter 51	
IP Table	447
51.1 IP Table Overview	447

51.2 Viewing the IP Table	448
Chapter 52	
ARP Table	451
52.1 ARP Table Overview	451
52.1.1 How ARP Works	451
52.2 The ARP Table Screen	452
Chapter 53	
Routing Table	453
53.1 Overview	453
53.2 Viewing the Routing Table Status	453
Chapter 54	
Configure Clone	455
54.1 Configure Clone	455
Chapter 55	
Troubleshooting.....	457
55.1 Power, Hardware Connections, and LEDs	457
55.2 Switch Access and Login	458
55.3 Switch Configuration	461
Chapter 56	
Product Specifications	463
Appendix A Common Services.....	473
Appendix B Legal Information	477
Index.....	481

PART I

User's Guide

Getting to Know Your Switch

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

1.1 Introduction

Your Switch is a stand-alone, layer-3, Gigabit Ethernet (GbE) switch with support for an optional 2-port 10 Gigabit uplink module. The XGS-4528F or XGS-4728F also provides two 12 Gigabit stacking ports. By integrating router functions, the Switch performs wire-speed layer-3 routing in addition to layer-2 switching.

The XGS-4526 comes with 20 100/1000 Mbps Ethernet ports and 4 GbE dual personality interfaces. The XGS-4528F or XGS-4728F comes with 24 GbE dual personality interfaces. A dual personality interface includes one Gigabit port and one slot for a mini-GBIC transceiver (SFP module) with one port active at a time.

The XGS-4526 requires 100 VAC to 240 VAC, 0.8 A power.

There are two XGS-4528F or XGS-4728F models. The XGS-4528F or XGS-4728F DC model requires DC power supply input of -36 VDC to -72 VDC, 1.5 A Max no tolerance. The XGS-4528F or XGS-4728F AC model requires 100 VAC to 240 VAC, 0.8 A power.

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

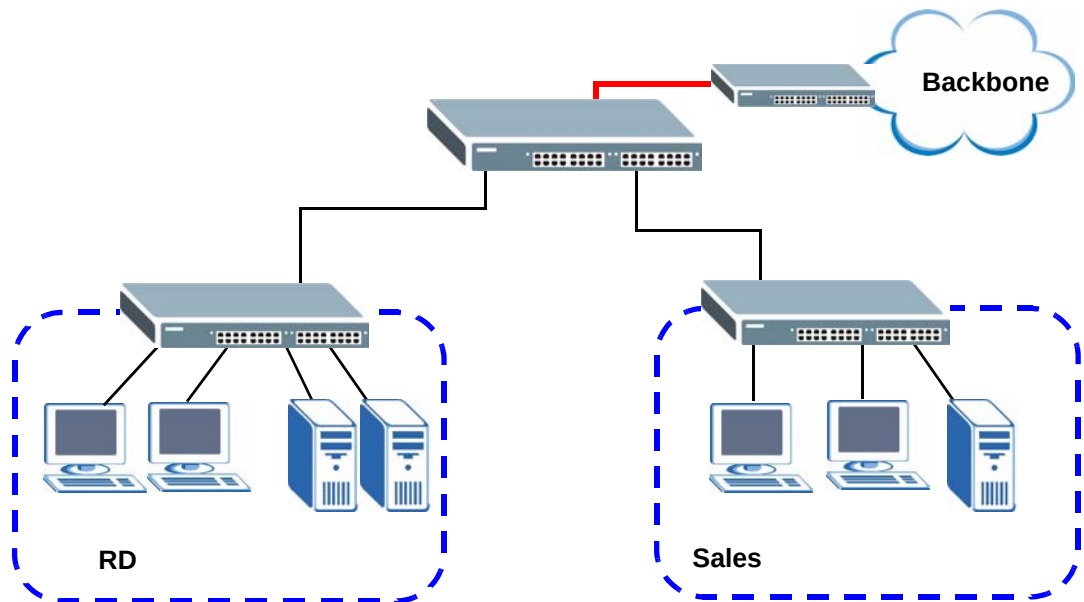
See [Chapter 56 on page 463](#) for a full list of software features available on the Switch.

1.1.1 Bridging Example

In this example the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a

super-fast uplink connection by using the optional 10 Gigabit uplink module on the Switch.

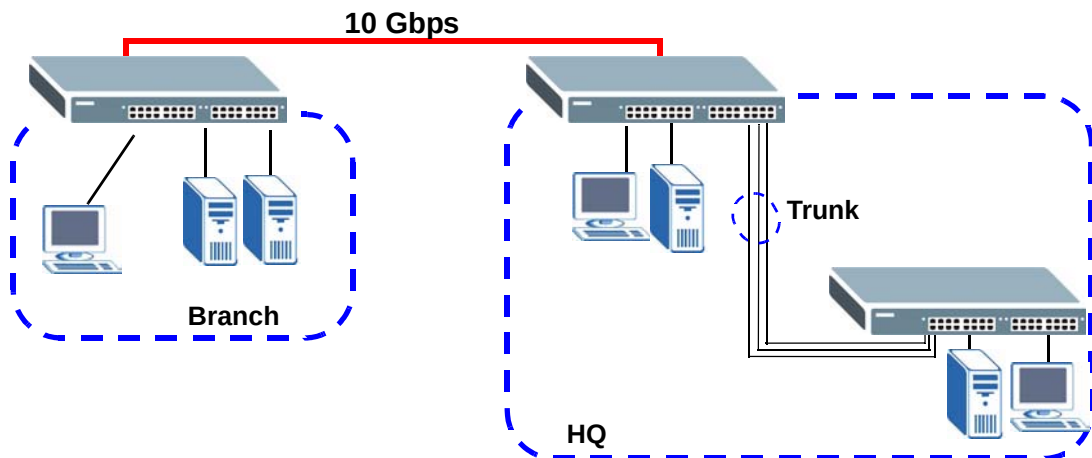
Figure 1 Bridging Application



1.1.2 High Performance Switching Example

The Switch is ideal for connecting two geographically dispersed networks that need high bandwidth. In the following example, a company uses the optional 10 Gigabit uplink modules to connect the headquarters to a branch office network. Within the headquarters network, a company can use trunking to group several physical ports into one logical higher-capacity link. Trunking can be used if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

Figure 2 High Performance Switching

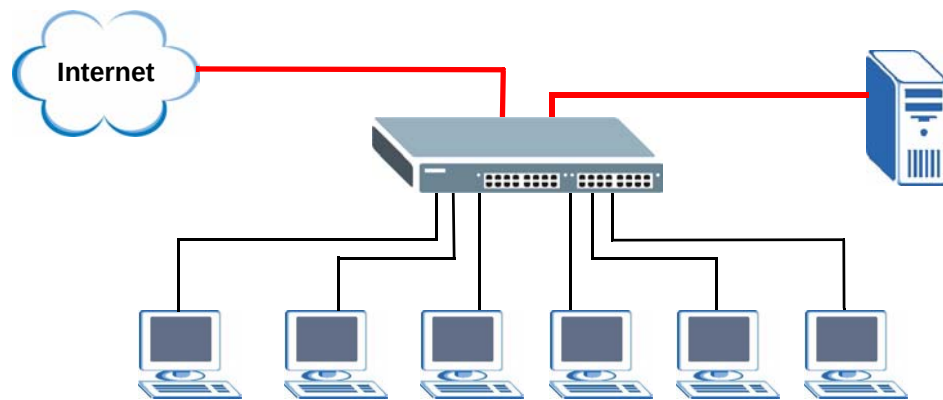


1.1.3 Gigabit Ethernet to the Desktop

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

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

Figure 3 Gigabit to the Desktop



1.1.4 IEEE 802.1Q VLAN Application Example

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

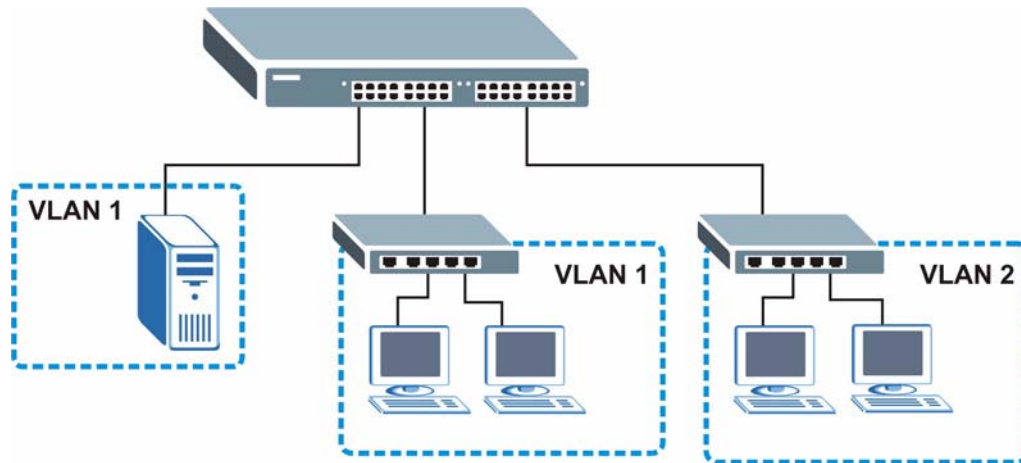
For more information on VLANs, refer to [Chapter 9 on page 117](#).

1.1.4.1 Tag-based VLAN Example

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

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

Figure 4 Shared Server Using VLAN Example



1.1.5 IPv6 Support

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses. At the time of writing, the Switch supports the following features.

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

For more information on IPv6, refer to the CLI Reference Guide.

1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See [Chapter 4 on page 47](#).
- Command Line Interface. Line commands offer an alternative to the Web Configurator and may be necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See [Section 45.8 on page 393](#).
- SNMP. The device can be monitored and/or managed by an SNMP manager. See [Section 46.3 on page 398](#).

1.3 Good Habits for Managing the Switch

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

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

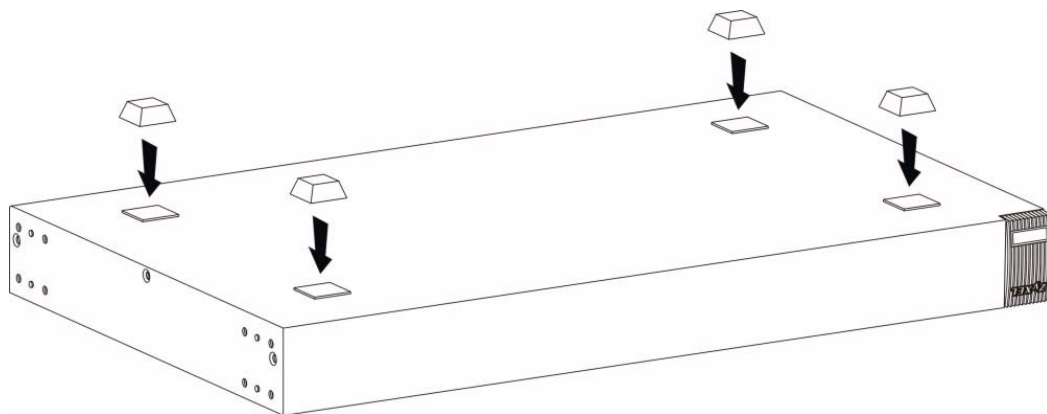
Hardware Installation and Connection

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

2.1 Freestanding Installation

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

Figure 5 Attaching Rubber Feet



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

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

2.2 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps.

2.2.1 Rack-mounted Installation Requirements

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

Failure to use the proper screws may damage the unit.

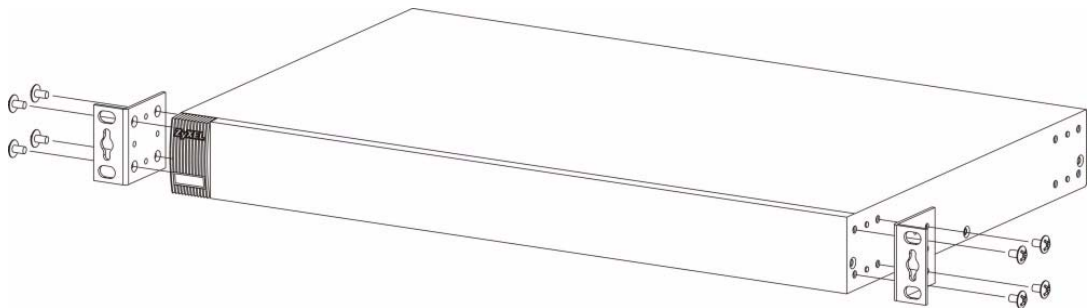
2.2.1.1 Precautions

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

2.2.2 Attaching the Mounting Brackets to the Switch

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

Figure 6 Attaching the Mounting Brackets

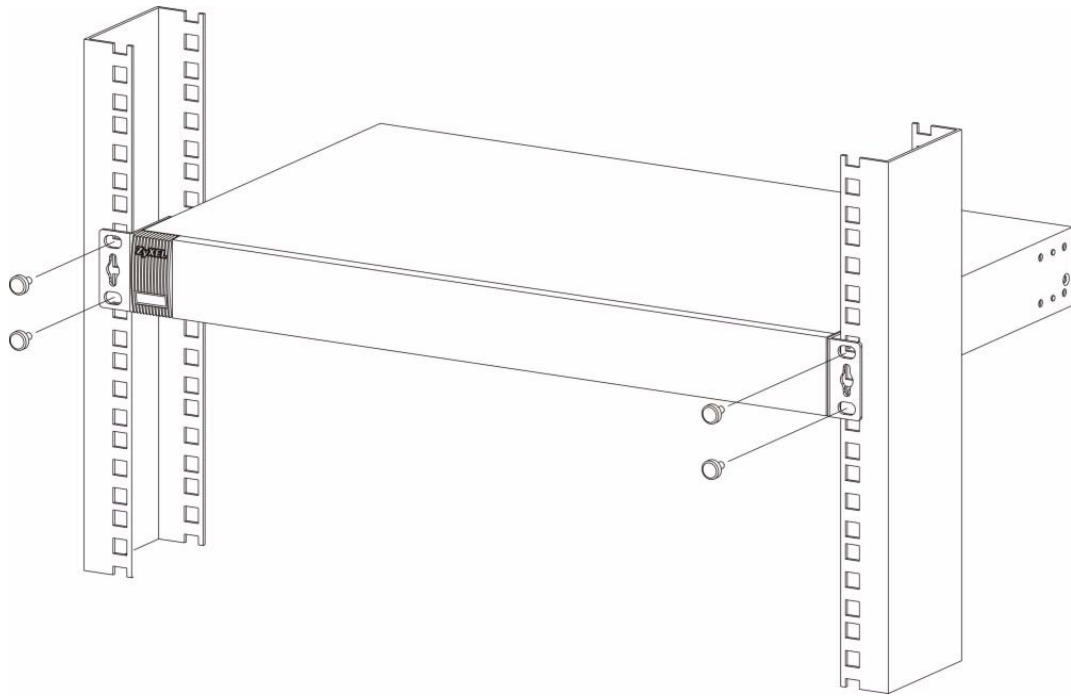


- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.
- 4 You may now mount the Switch on a rack. Proceed to the next section.

2.2.3 Mounting the Switch on a Rack

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

Figure 7 Mounting the Switch on a Rack



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

Hardware Overview

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

3.1 Front Panel Connections

The figure below shows the front panel of the Switch.

Figure 8 Front Panel: XGS-4526

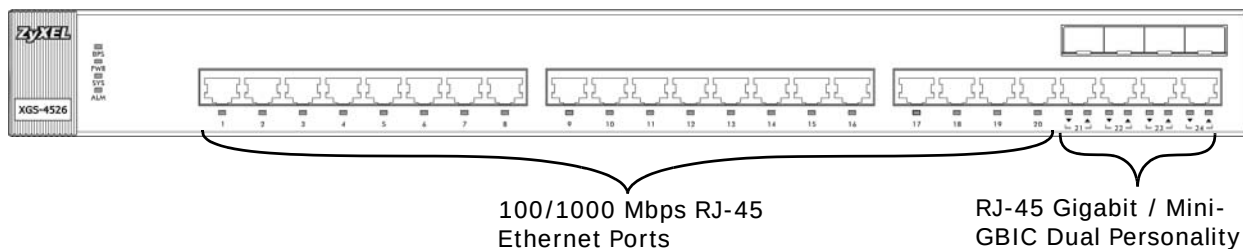


Figure 9 Front Panel: XGS-4528F

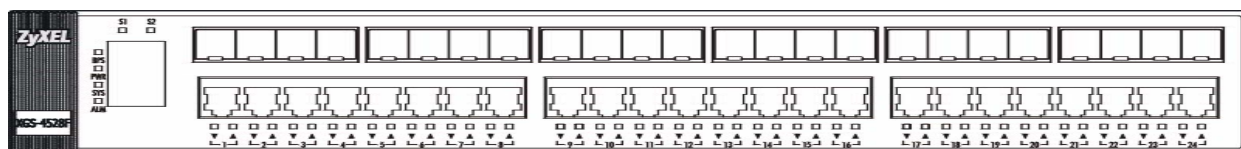
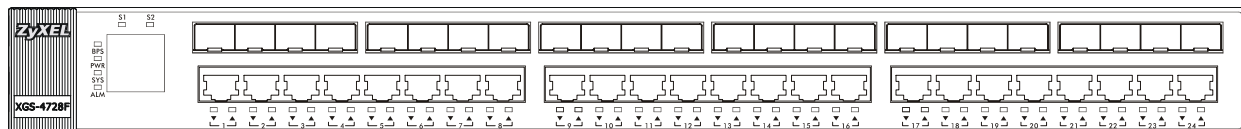


Figure 10 Front Panel: XGS-4728F



The following table describes the ports.

Table 1 Panel Connections

CONNECTOR	DESCRIPTION
20 100/1000 Mbps RJ-45 Ethernet Ports (XGS-4526 only)	Connect these ports to a computer, a hub, an Ethernet switch or router.
4 or 24 Dual Personality Interfaces	Each interface has one 1000Base-T copper RJ-45 port and one mini-GBIC (Gigabit Interface Converter) fiber port, with one port active at a time.
	4 or 24 1000Base-T Ports: Connect these ports to high-bandwidth backbone network Ethernet switches using Category 5/5e/6 1000Base-T Ethernet cables. Use an 8-wire Ethernet cable for Gigabit connections. Using a 4-wire Ethernet cable limits your connection to 100 Mbps. Note that the connection speed also depends on what the Ethernet device at the other end can support.
	4 or 24 Mini-GBIC Ports: Use Small Form-Factor Pluggable (SFP) transceivers in these ports for 1000Base-X fiber-optic connections to backbone Ethernet switches.

3.1.1 Dual Personality Interfaces

There are 4 or 24 Dual Personality interfaces, comprising 4 or 24 1000Base-T/mini-GBIC combo ports. For each interface you can connect either to the 1000Base-T port or the mini-GBIC port. The mini-GBIC ports have priority over the 1000Base-T ports. This means that if a mini-GBIC port and the corresponding 1000Base-T port are connected at the same time, the 1000Base-T port will be disabled.

3.1.2 1000Base-T Ports

The Switch has 24 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 100/1000 Mbps Gigabit Ethernet, the speed can be 100 Mbps or 1000 Mbps. The duplex mode can be both half or full duplex at 100 Mbps and full duplex only at 1000 Mbps.

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

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

3.1.2.1 Default Ethernet Settings

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

- Speed: Auto
- Duplex: Auto
- Flow control: Off

3.1.3 Mini-GBIC Slots

These are 4 or 24 slots for Small Form-Factor Pluggable (SFP) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the Switch. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-Factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

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

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

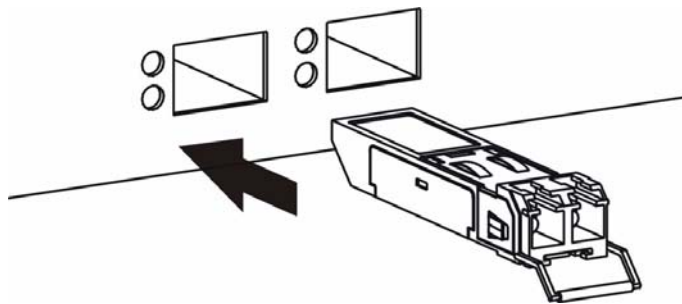
To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.3.1 Transceiver Installation

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

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

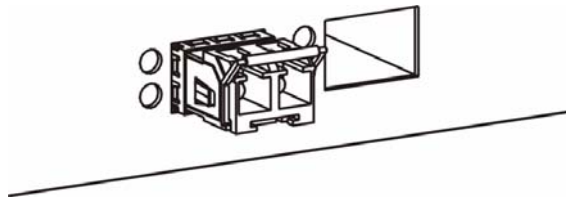
Figure 11 Transceiver Installation Example



- 2 Press the transceiver firmly until it clicks into place.

- 3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 12 Installed Transceiver

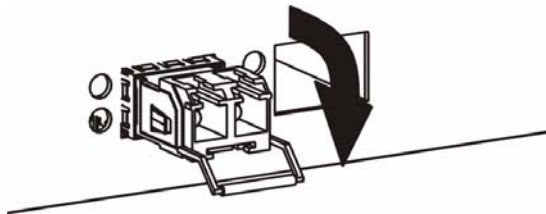


3.1.3.2 Transceiver Removal

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

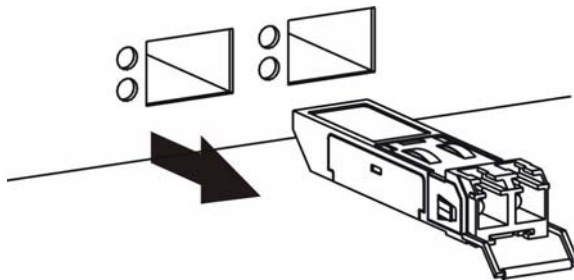
- 1 Open the transceiver's latch (latch styles vary).

Figure 13 Opening the Transceiver's Latch Example



- 2 Pull the transceiver out of the slot.

Figure 14 Transceiver Removal Example

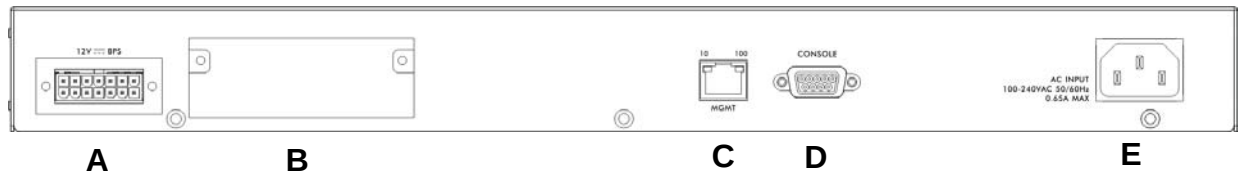


3.2 Rear Panel

3.2.1 XGS-4526

The following figure shows the rear panel of the Switch.

Figure 15 Rear Panel



The rear panel contains:

- A connector for the backup power supply (**A**)
- An optional slot (**B**) for installing an EM-422 or EM-412 uplink module
- An RJ-45 out-of-band management port (**C**)
- An RS-232 management console port (**D**)
- A connector for the power receptacle (**E**)

3.2.2 XGS-4528F or XGS-4728F

The following figures show the rear panels of the AC and DC power input model switches. The rear panels contain:

- A connector for the backup power supply (**A**)
- An optional slot (**B**) for installing an EM-422 or EM-412 uplink module
- Two stacking ports (**C**)
- An RJ-45 out-of-band management port (**D**)
- An RS-232 management console port (**E**)
- A connector for the power receptacle (**F**)
- A power switch (**G**) (DC power input model only).

Figure 16 Rear Panel - AC Model

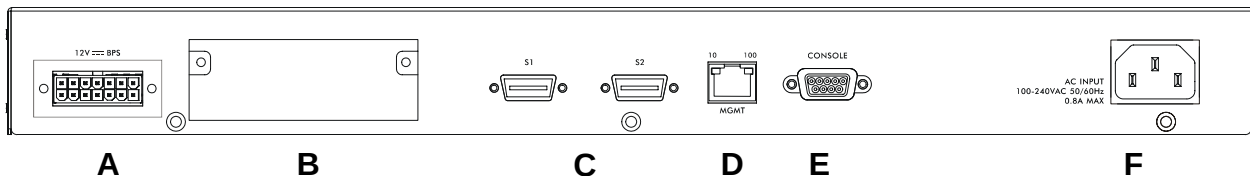
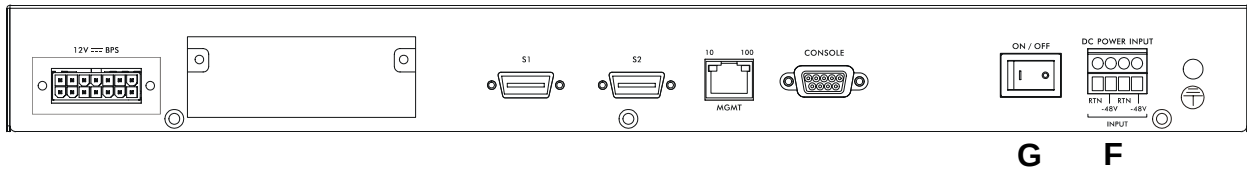
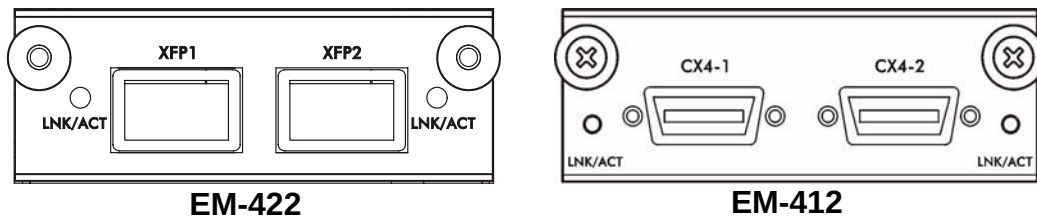


Figure 17 Rear Panel - DC Model

3.2.3 Uplink Module

The following figure shows the front panel of the EM-422 and EM-412 modules.

Figure 18 The Front Panel of the EM-422 and EM-412 Modules

3.2.4 Rear Panel Connections

The following table describes the ports on the rear panel.

Table 2 Panel Connections

CONNECTOR	DESCRIPTION
Optional two XFP or CX4 Ports	These ports are available when you install an EM-422 or ES-412 in the optional uplink module (B in the figure above). Both the EM-422 and ES-412 are used to connect your switch to other high-speed Ethernet switches for stacking in you network. - For EM-422 connection: Use 10 Gigabit Small Form Factor Pluggable (XFP) transceivers to connect 1000Base-X fiber-optic cables to these ports. See Section 3.1.3.1 on page 39 and Section 3.1.3.2 on page 40 for information on installing and removing transceivers. - For EM-412 connection: Use 10GBase-CX4 cables to connect to these ports. See the EM-422 and EM-412 User's Guides for more information.
Two stacking ports (XGS-4528F or XGS-4728F)	Connect these ports to other XGS-4528F or XGS-4728F switches for stacking using stacking cables.
Management Port	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the Switch.
Console Port	Only connect this port to your computer (using an RS-232 cable) if you want to configure the Switch using the command line interface (CLI) via the console port.

3.2.5 Power Connector

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

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

Note: Check the power supply requirements in [Chapter 56 on page 463](#), and make sure you are using an appropriate power source.

Keep the power supply switch and the Switch's power switch in the OFF position until you come to the procedure for turning on the power.

Use only power wires of the required diameter for connecting the Switch to a power supply.

3.2.5.1 AC Power Connection

Note: This is only for the AC model of the Switch.

Connect the female end of the power cord to the power socket of your Switch. Connect the other end of the cord to a power outlet.

3.2.5.2 DC Power Connection

Note: This is only for the DC model of the Switch.

The Switch uses a single ETB series terminal block plug with four pins which allows you to connect up to two separate power supplies. If one power supply fails the system can operate on the remaining power supply. Use two wires to connect to a single terminal pair, one wire for the positive terminal and one wire for the negative terminal.

Note: The current rating of the power wires must be greater than 20 Amps. The power supply to which the Switch connects must have a built-in circuit breaker or switch to toggle the power.

Note: When installing the power wire, push it wire firmly into the terminal as deep as possible and make sure that no exposed (bare) wire can be seen or touched.

Exposed power wire is dangerous. Use extreme care when connecting a DC power source to the device.

To connect a power supply:

- 1 Use a screwdriver to loosen the terminal block captive screws.
- 2 Connect one end of a power wire to the Switch's **RTN** (return) pin and tighten the captive screw.
- 3 Connect the other end of the power wire to the positive terminal on the power supply.
- 4 Connect one end of a power wire to the Switch's **-48V** (input) pin and tighten the captive screw.
- 5 Connect the other end of the power wire to the negative terminal on the power supply.
- 6 Insert the terminal block plug in the Switch's terminal block header.

3.2.6 External Backup Power Supply Connector

The Switch supports external backup power supply (BPS).

The Switch constantly monitors the status of the internal power supply. The backup power supply automatically provides power to the Switch in the event of a power failure. Once the Switch receives power from the backup power supply, it will not automatically switch back to using the internal power supply even when the power is resumed.

3.2.7 Console Port

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

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the RS-232 console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.3 LEDs

The following table describes the LEDs.

Table 3 LEDs

LED	COLO R	STATUS	DESCRIPTION
BPS	Green	Blinking	The system is receiving power from the backup power supply.
		On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/ malfunctioning.
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
S1 (XGS-4528F or XGS-4728F)	Green	On	The Switch is connected to other switches in the stack on Stacking Port 1.
		Off	The Switch is not connected to other switches in the stack on Stacking Port 1.
S2 (XGS-4528F or XGS-4728F)	Green	On	The Switch is connected to other switches in the stack on Stacking Port 2.
		Off	The Switch is not connected to other switches in the stack on Stacking Port 2.
System Status		Displays hourglass icon	The Switch is starting up.
		Displays Stack ID number	The LED is showing the Stack ID number of the Switch.
1000Base-T Gigabit Ports (▼)			
1-24	Green	Blinking	The system is transmitting/receiving to/from a 10/1000 Mbps Ethernet network.
		On	The link to a 10/1000 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
1000Base-X Mini-GBIC Slots (▲)			

Table 3 LEDs (continued)

LED	COLO R	STATUS	DESCRIPTION
1-24 or 21-24	Green	On	The port has a successful connection.
		Blinking	The port is receiving or transmitting data.
		Off	This link is disconnected.

The Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Firefox 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

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

4.2 System Login

- 1 Start your web browser.
- 2 Type “http://” and the IP address of the Switch (for example, the default management IP address is 192.168.1.1 through an in-band (non-**MGMT**) port and 192.168.0.1 through the **MGMT** port) in the Location or Address field. Press [ENTER].

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

Figure 19 Web Configurator: Login



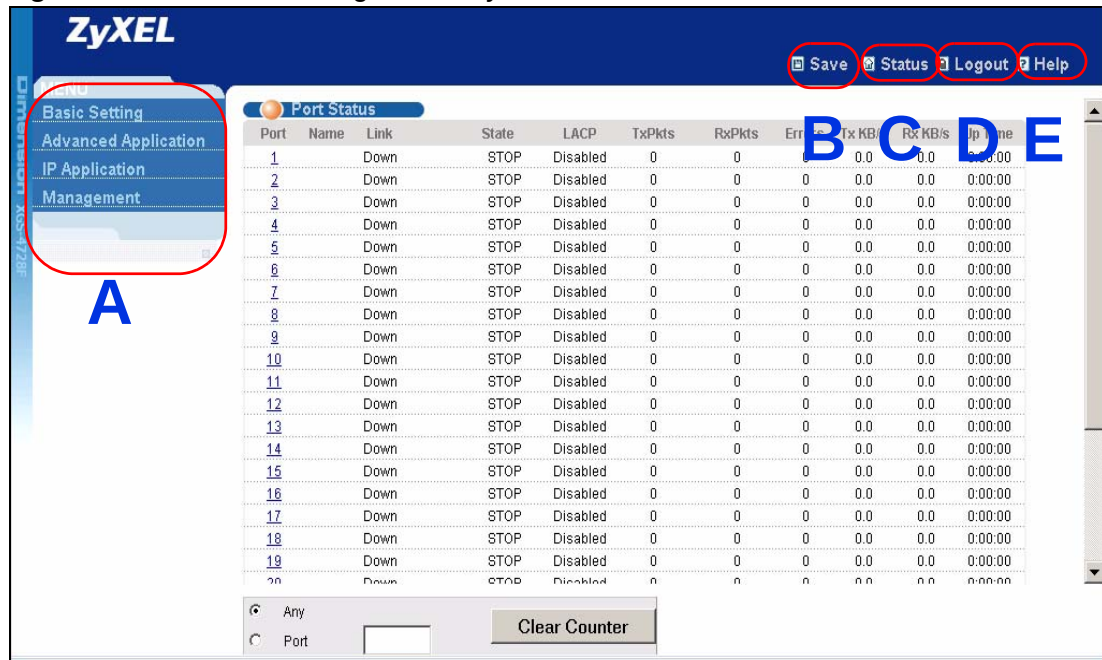
- 4 Click **OK** to view the first web configurator screen.

4.3 The Web Configurator Layout

The **Status** screen is the first screen that displays when you access the web configurator. This guide uses the XGS-4728F screens as an example. The screens may vary slightly for different models.

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

Figure 20 The Web Configurator Layout



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

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

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is saved in the configuration file from which the Switch booted from and it stays the same even if the Switch's power is turned off. See [Section 45.3 on page 390](#) for information on saving your settings to a specific configuration file.

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

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

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

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

Table 4 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information and time settings for the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, MAC address learning, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to screens where you can configure speed, flow control and priority settings for individual Switch ports.
Advanced Application	

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed on a port.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the Switch.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to screens where you can activate and configure VLAN stacking.
Multicast	This link takes you to screen where you can configure various multicast features, IGMP snooping and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication, authorization and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
VLAN Mapping	This link takes you to screens where you can configure VLAN mapping settings on the Switch.
Layer 2 Protocol Tunneling	This link takes you to a screen where you can configure L2PT (Layer 2 Protocol Tunneling) settings on the Switch.
sFlow	This link takes you to screens where you can configure sFlow settings on the Switch.
PPPoE	This link takes you to screens where you can configure how the Switch gives a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.
Errdisable	This link takes you to a screen where you can configure CPU protection and error disable recovery.
Private VLAN	This link takes you to a screen where you can block traffic between ports in a VLAN on the Switch.
IP Application	
Static Route	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
Policy Routing	This link takes you to screens where you can configure policy routing rules.
RIP	This link takes you to a screen where you can configure the RIP (Routing Information Protocol) direction and versions.
OSPF	This link takes you to screens where you can view the OSPF status and configure OSPF settings.
IGMP	This link takes you to a screen where you can configure the IGMP settings.
DVMRP	This link takes you to a screen where you can configure the DVMRP (Distance Vector Multicast Routing Protocol) settings.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
ARP Learning	This link takes you to a screen where you can configure ARP learning mode on a per-port basis.
Load Sharing	This link takes you to a screen where you can enable Equal-Cost MultiPath (ECMP) routing and set the criteria the Switch uses to determine the routing path for a packet.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to screens where you can view system logs and can test port(s).

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of MAC address it is.
IP Table	This link takes you to a screen where you can view the IP addresses and VLAN ID of a device attached to a port. You can also view what kind of device it is.
ARP Table	This link takes you to a screen where you can view the MAC address – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to (an)other port(s).

4.3.1 Change Your Password

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

Figure 21 Change Administrator Login Password

Logins Access Control

Administrator

Old Password

New Password

Retype to confirm

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

Edit Logins

Login	User Name	Password	Retype to confirm
1			
2			
3			
4			

4.4 Saving Your Configuration

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

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

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

4.5 Switch Lockout

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

- 1 Delete the management VLAN (default is VLAN 1).
- 2 Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
- 3 Filter all traffic to the CPU port.
- 4 Disable all ports.
- 5 Misconfigure the text configuration file.
- 6 Forget the password and/or IP address.
- 7 Prevent all services from accessing the Switch.
- 8 Change a service port number but forget it.

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

4.6 Resetting the Switch

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

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

- 1 Connect to the console port using a computer with terminal emulation software. See [Section 3.2 on page 41](#) for details.
- 2 Disconnect and reconnect the Switch's power to begin a session. When you reconnect the Switch's power, you will see the initial screen.
- 3 When you see the message “Press any key to enter Debug Mode within 3 seconds ...” press any key to enter debug mode.
- 4 Type `atlc` after the “Enter Debug Mode” message.
- 5 Wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.
- 6 After a configuration file upload, type `atgo` to restart the Switch.

Figure 22 Resetting the Switch: Via the Console Port

```

Bootbase Version: V1.00 | 10/22/2007 12:48:50
RAM:Size = 128 Mbytes
DRAM POST: Testing:131072K OK
DRAM Test SUCCESS !
FLASH: Intel 64M

ZyNOS Version: V4.00(BBC.0)b1 | 10/14/2010 17:32:18

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

```

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

4.7 Logging Out of the Web Configurator

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

Figure 23 Web Configurator: Logout Screen



4.8 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

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

Initial Setup Example

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

5.1 Overview

The following lists the configuration steps for the example network:

- Configure an IP interface
- Configure DHCP server settings
- Create a VLAN
- Set port VLAN ID
- Enable RIP

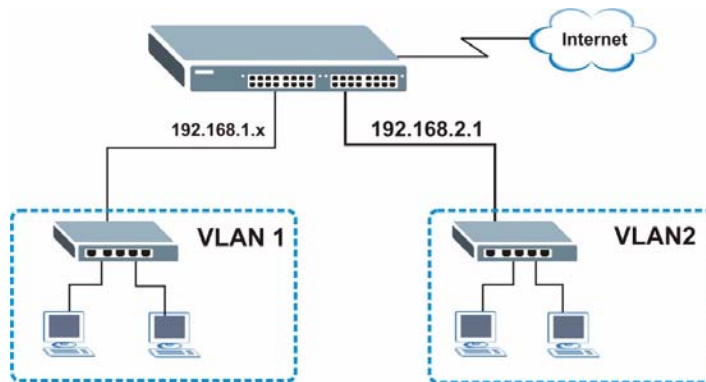
5.1.1 Configuring an IP Interface

On a layer-3 switch, an IP interface (also known as an IP routing domain) is not bound to a physical port. The default IP address of the Switch is 192.168.1.1 with a subnet mask of 255.255.255.0.

In the example network, since the **RD** network is already in the same IP interface as the Switch, you don't need to create an IP interface for it. However, if you want to have the **Sales** network on a different routing domain, you need to create a

new IP interface. This allows the Switch to route traffic between the **RD** and **Sales** networks.

Figure 24 Initial Setup Network Example: IP Interface



- 1 Connect your computer to the **MGMT** port that is used only for management. Make sure your computer is in the same subnet as the **MGMT** port.
- 2 Open your web browser and enter 192.168.0.1 (the default **MGMT** port IP address) in the address bar to access the web configurator. See [Section 4.2 on page 47](#) for more information.
- 3 Click **Basic Setting** and **IP Setup** in the navigation panel.
- 4 Configure the related fields in the **IP Setup** screen.

IP Setup

Default Gateway: 0.0.0.0
 Domain Name Server: 0.0.0.0
 Default Management: ☒ In-band ☐ Out-of-band

Management IP Address

IP Address: 192.168.0.1
 IP Subnet Mask: 255.255.255.0
 Default Gateway: 0.0.0.0

Apply Cancel

IP Interface

IP Address: 192.168.2.1
 IP Subnet Mask: 255.255.255.0
 VID: 2

Add Cancel

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.12	255.255.255.0	1	☐

Delete Cancel

EXAMPLE

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

- 5 In the **VID** field, enter the ID of the VLAN group to which you want this IP interface to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 6 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 Configuring DHCP Server Settings

You can set the Switch to assign network information (such as the IP address, DNS server, etc.) to DHCP clients on the network.

For the example network, configure two DHCP client pools on the Switch for the DHCP clients in the **RD** and **Sales** networks.

- 1 In the web configurator, click **IP Application** and **DHCP** in the navigation panel and click the **VLAN** link.
- 2 In the **VLAN Setting** screen, specify the ID of the VLAN to which the DHCP clients belong, the starting IP address pool, subnet mask, default gateway address and the DNS server address(es).
- 3 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.

VLAN Setting Status

VID:

DHCP Status: ☒ Server ☐ Relay

Server

Client IP Pool Starting Address:

Size of Client IP Pool:

IP Subnet Mask:

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

Relay

Remote DHCP Server 1:

Remote DHCP Server 2:

Remote DHCP Server 3:

Relay Agent Information: ☐ Option 82

Information:

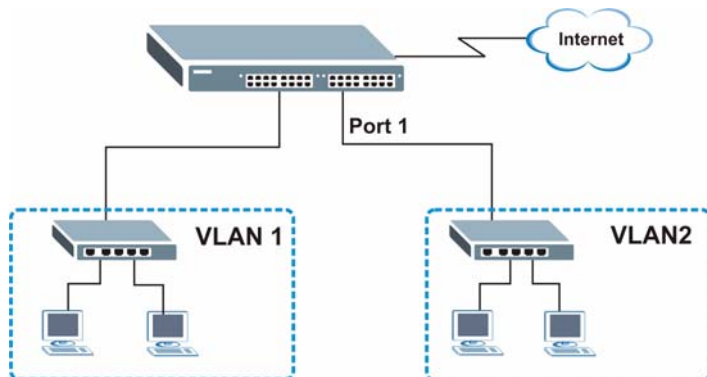
EXAMPLE

5.1.3 Creating a VLAN

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

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

Figure 25 Initial Setup Network Example: VLAN



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

Index	VID	Elapsed Time	Status
1	1	1:00:31	Static

- 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.

Port	Control	Tagging
1	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
2	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
3	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
4	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
5	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
6	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
7	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
8	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging

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

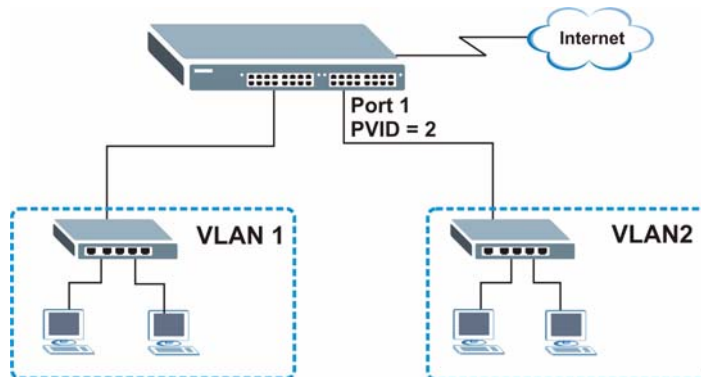
- 3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
- 4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch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

5.1.4 Setting Port VID

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

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

Figure 26 Initial Setup Network Example: Port VID



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

VLAN Port Setting						
Subnet Based Vlan Protocol Based Vlan VLAN Status						
GVRP ☐						
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	2	☐	All	☐	☐
2	☐	1	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐
5	☐	1	☐	All	☐	☐
6	☐	1	☐	All	☐	☐
7	☐	1	☐	All	☐	☐
8	☐	1	☐	All	☐	☐
9	☐	1	☐	All	☐	☐
10	☐	1	☐	All	☐	☐

EXAMPLE

5.1.5 Enabling RIP

To exchange routing information with other routing devices across different routing domains, enable RIP (Routing Information Protocol) in the **RIP** screen.

- 1 Click **IP Application** and **RIP** in the navigation panel.

- 2 Select **Both** in the **Direction** field to set the Switch to broadcast and receive routing information.

- 3 In the **Version** field, select **RIP-1** for the RIP packet format that is universally supported.

Index	Network	Direction	Version
1	192.168.1.1/24	Both	RIP-1

Apply Cancel **EXAMPLE**

- 4 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.

Tutorials

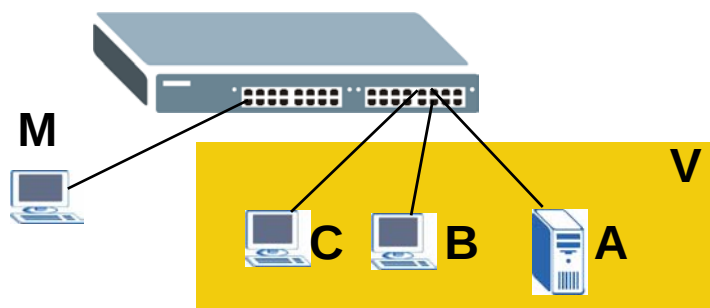
This chapter provides some examples of using the web configurator to set up and use the Switch. The tutorials include:

- [How to Use DHCP Snooping on the Switch](#)
- [How to Use DHCP Relay on the Switch](#)
- [How to Use PPPoE IA on the Switch](#)
- [How to Use Error Disable and Recovery on the Switch](#)
- [How to Set Up a Guest VLAN](#)
- [How to Do Port Isolation in a VLAN](#)
- [How to Configure Routing Policy](#)

6.1 How to Use DHCP Snooping on the Switch

You only want DHCP server **A** connected to port 5 to assign IP addresses to all devices in VLAN network (**V**). Create a VLAN containing ports 5, 6 and 7. Connect a computer **M** to the Switch's **MGMT** port.

Figure 27 Tutorial: DHCP Snooping Tutorial Overview



Note: For related information about DHCP snooping, see [Section 26.1 on page 259](#).

The settings in this tutorial are as the following.

Table 6 Settings in this Tutorial

HOST	PORT CONNECTED	VLAN	PVID	DHCP SNOOPING PORT TRUSTED
DHCP Server (A)	5	1 and 100	100	Yes
DHCP Client (B)	6	1 and 100	100	No
DHCP Client (C)	7	1 and 100	100	No

- 1 Access the Switch from the **MGMT** port through **http://192.168.0.1** by default. Log into the Switch by entering the username (default: **admin**) and password (default: **1234**).
- 2 Go to **Advanced Application > VLAN > Static VLAN**, and create a VLAN with ID of 100. Add ports 5, 6 and 7 in the VLAN by selecting **Fixed** in the **Control** field as shown.

Deselect **Tx Tagging** because you don't want outgoing traffic to contain this VLAN tag.

Click **Add**.

Static VLAN VLAN Status

☒ **ACTIVE**

Name:

VLAN Group ID:

Port	Control	Tagging
*	Normal	☒ Tx Tagging
1	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
2	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
3	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
4	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
5	☐ Normal ☒ Fixed ☐ Forbidden	☐ Tx Tagging
6	☐ Normal ☒ Fixed ☐ Forbidden	☐ Tx Tagging
7	☐ Normal ☒ Fixed ☐ Forbidden	☐ Tx Tagging
8	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging

☒ Normal ☐ Fixed ☐ Forbidden ☒ Tx Tagging

- 3 Go to **Advanced Application > VLAN > VLAN Port Setting**, and set the PVID of the ports 5, 6 and 7 to 100. This tags untagged incoming frames on ports 5, 6 and 7 with the tag 100.

VLAN Port Setting Subnet Based Vlan Protocol Based Vlan VLAN Status

GVRP ☐

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	1	☐	All	☐	☐
2	☐	1	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐
5	☐	100	☐	All	☐	☐
6	☐	100	☐	All	☐	☐
7	☐	100	☐	All	☐	☐
8	☐	1	☐	All	☐	☐

Apply Cancel

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

DHCP Snooping Configure Port VLAN DHCP Snooping

Active ☒

DHCP Vlan ☐ Disable ☒ 100

Database

Agent URL

Timeout interval seconds

Write delay interval seconds

Renew DHCP Snooping URL Renew

Apply Cancel

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

Port VLAN DHCP Snooping

- 6 The **DHCP Snooping Port Configure** screen appears. Select **Trusted** in the **Server Trusted state** field for port 5 because the DHCP server is connected to port 5. Keep ports 6 and 7 **Untrusted** because they are connected to DHCP clients. Click **Apply**.

Port	Server Trusted state	Rate (pps)
*	Untrusted	
1	Untrusted	0
2	Untrusted	0
3	Untrusted	0
4	Untrusted	0
5	Trusted	0
6	Untrusted	0
7	Untrusted	0
8	Untrusted	0
9	Untrusted	0

Apply Cancel

- 7 Go to **Advanced Application > IP Source Guard > 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 the **Option82** and **Information** fields in the entry. See [Section 26.1.1.3 on page 261](#).

Show VLAN Start VID 100 End VID 100

Apply

VID	Enabled	Option82	Information
*	No	☐	☐
100	Yes	☐	☐

Apply Cancel

- 8 Click **Save** at the top right corner of the web configurator to save the configuration permanently.



- 9 Connect your DHCP server to port 5 and a computer (as DHCP client) to either port 6 or 7. The computer should be able to get an IP address from the DHCP server. If you put the DHCP server on port 6 or 7, 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**, you should see an IP assignment with the type **dhcp-snooping** as shown.

IP Source Guard						
Static Binding DHCP Snooping ARP Inspection						
Index	MAC Address	IP Address	Lease	Type	VID	Port
1	00:02:00:00:00:1c	10.10.1.16	6d23h17m 0s	dhcp-snooping	100	7

You can also telnet or log into the Switch's console. 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	7	
Total number of bindings: 1						

6.2 How to Use DHCP Relay on the Switch

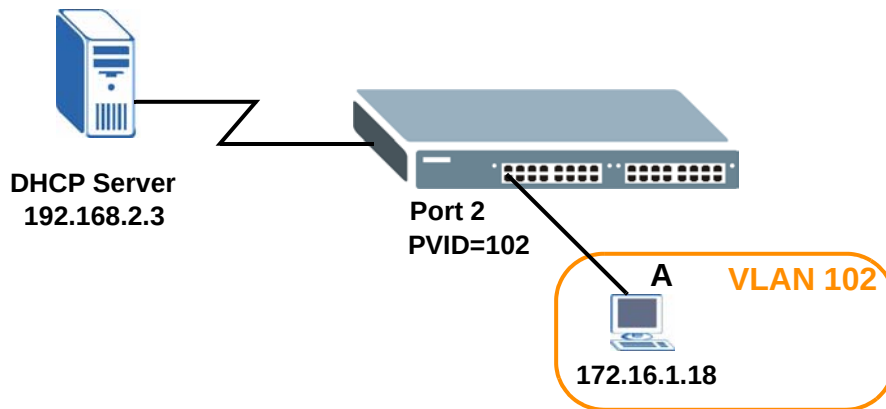
This tutorial describes how to configure your Switch to forward DHCP client requests to a specific DHCP server. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

6.2.1 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) and gateway information 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 28 Tutorial: DHCP Relay Scenario



6.2.2 Creating 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.

The screenshot shows the 'Switch Setup' web interface. The 'VLAN Type' is set to '802.1Q' (selected with a radio button). Below it, 'Bridge Control Protocol Transparency' is set to 'Active'. The 'MAC Address Learning' section includes 'Aging Time' (300 seconds), 'Join Timer' (200 milliseconds), 'Leave Timer' (600 milliseconds), and 'Leave All Timer' (10000 milliseconds). The 'Priority Queue Assignment' section shows a list of levels from level7 to level0 with corresponding values in dropdown menus: level7 (7), level6 (6), level5 (5), level4 (4), level3 (3), level2 (1), level1 (0), and level0 (2). At the bottom, there are 'Apply' and 'Cancel' buttons.

- 3 Click **Advanced Application > VLAN > Static VLAN**.

- 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.

Static VLAN VLAN Status

ACTIVE ☒

Name

VLAN Group ID

Port	Control			Tagging
*	Normal			☒ Tx Tagging
1	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
2	☐ Normal	☒ Fixed	☐ Forbidden	☐ Tx Tagging
3	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
4	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
5	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
24	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
25	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
26	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
27	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
28	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging

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

VLAN Status **VLAN Port Setting** Static VLAN

VLAN Search by VID Search

The Number of VLAN: 2.

Index	VID	Elapsed Time	Status
1	1	49:52:07	Static
2	102	0:00:15	Static

Change Pages Previous Next

- 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.

VLAN Port Setting Subnet Based Vlan Protocol Based Vlan VLAN Status

GVRP ☐

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	1	☐	All	☐	☐
2	☐	102	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐
5	☐	1	☐	All	☐	☐
6	☐	1	☐	All	☐	☐
7	☐	1	☐	All	☐	☐

Apply Cancel

- 11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

6.2.3 Configuring DHCP 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** 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 the **Option 82** and the **Information** check boxes.
- 5 Click **Apply** to save your changes back to the run-time memory.

DHCP Relay		Status
Active	☒	
Remote DHCP Server 1	192.168.2.3	
Remote DHCP Server 2	0.0.0.0	
Remote DHCP Server 3	0.0.0.0	
Relay Agent Information	☒ Option 82	
Information	☒ XGS-4728F	
Apply Cancel		

- 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.

6.2.4 Troubleshooting

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

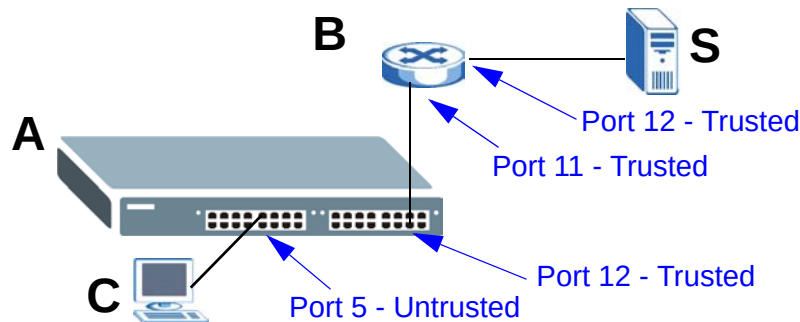
- 1 Client **A** is connected to the Switch's port 2 in VLAN 102.
- 2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.

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

6.3 How to Use PPPoE IA on the Switch

You want to configure PPPoE Intermediate Agent on the Switch (**A**) to pass a subscriber's information to a PPPoE server (**S**). There is another switch (**B**) between switch **A** and server **S**. Switch **B** is connected to switch **A**. In this way, PPPoE server **S** can identify subscriber **C** and may apply different settings to it.

Figure 29 Tutorial: PPPoE Intermediate Agent Tutorial Overview



Note: For related information about PPPoE IA, see [Section 31.3 on page 302](#).

The settings in this tutorial are as follows:

Table 7 Settings in this Tutorial

SWITCH	PORT CONNECTED	VLAN	CIRCUIT-ID	REMOTE-ID	PPPOE IA PORT TRUSTED
A	Port 5 (to C)	1	userC	00134900000A	Untrusted
	Port 12 (to B)	1	N/A	N/A	Trusted
B	Port 11 (to A)	1	N/A	N/A	Trusted
	Port 12 (to S)	1	N/A	N/A	Trusted

6.3.1 Configuring Switch A

- 1 Click **Advanced Application > PPPoE > Intermediate Agent**. Select **Active** then click **Apply**.

Intermediate Agent Port VLAN PPPoE

Active ☒

access-node-identifier XGS-4728F

circuit-id

Active ☐

identifier-string

option spv

delimiter /

Apply Cancel

Click **Port** on the top of the screen.

- 2 Select **Untrusted** for port 5 and enter **userC** as **Circuit-id** and **00134900000A** as **Remote-id**.

Select **Trusted** for port 12 and then leave the other fields empty. Click **Apply**.

Port VLAN Intermediate Agent

Port	Server Trusted State	Circuit-id	Remote-id
*	Untrusted		
1	Untrusted		
2	Untrusted		
3	Untrusted		
4	Untrusted		
5	Untrusted	userC	00134900000A
6	Untrusted		
7	Untrusted		
8	Untrusted		
9	Untrusted		
10	Untrusted		
11	Untrusted		
12	Trusted		
13	Untrusted		
14	Untrusted		

Then Click **Intermediate Agent** on the top of the screen.

- 3 The **Intermediate Agent** screen appears. Click **VLAN** on the top of the screen.

The screenshot shows the 'Intermediate Agent' configuration window. At the top, there are three tabs: 'Intermediate Agent', 'Port', and 'VLAN'. The 'VLAN' tab is selected and circled in red. Below the tabs, there are two main sections. The first section has an 'Active' checkbox checked and an 'access-node-identifier' field containing 'XGS-4728F'. The second section is titled 'circuit-id' and contains an 'Active' checkbox (unchecked), an 'identifier-string' field, an 'option' dropdown menu set to 'spv', and a 'delimiter' dropdown menu set to '/'. At the bottom of the window are 'Apply' and 'Cancel' buttons.

- 4 Enter 1 for both **Start VID** and **End VID** since both the Switch and PPPoE server are in VLAN 1 in this example. Click **Apply**.

The screenshot shows the 'VLAN' configuration window. At the top, there are two tabs: 'VLAN' and 'Intermediate Agent'. The 'VLAN' tab is selected. Below the tabs, there is a 'Show VLAN' checkbox, a 'Start VID' field containing '1', and an 'End VID' field containing '1'. These three elements are grouped together and circled in red. Below this group is an 'Apply' button. At the bottom of the window is a table with four columns: 'VID', 'Enabled', 'Circuit-id', and 'Remote-id'. The first row of the table has a '*' in the 'VID' column, 'No' in the 'Enabled' column (with a dropdown arrow), and empty checkboxes in the 'Circuit-id' and 'Remote-id' columns. At the bottom of the window are 'Apply' and 'Cancel' buttons.

- Then select **Yes** to enable PPPoE IA in VLAN 1 and also select **Circuit-id** and **Remote-id** to allow the Switch to add these two strings to frames tagged with VLAN 1 and pass to the PPPoE server. Click **Apply**.

The screenshot shows the 'VLAN' configuration page with the 'Intermediate Agent' tab selected. At the top, there are fields for 'Start VID' and 'End VID', and a 'Show VLAN' button. Below these is an 'Apply' button. A table lists VLAN configurations:

VID	Enabled	Circuit-id	Remote-id
*	No	☐	☐
1	Yes	☒	☒

The row for VID 1 is highlighted with a red circle. At the bottom, there are 'Apply' and 'Cancel' buttons.

6.3.2 Configuring Switch B

The example uses another XGS-4728F as switch **B**.

- Click **Advanced Application > PPPoE > Intermediate Agent**. Select **Active** then click **Apply**.

The screenshot shows the 'Intermediate Agent' configuration page under the 'PPPoE' tab. The 'Active' checkbox is checked and circled in red. Below it, the 'access-node-identifier' is set to 'XGS-4728F'. The 'circuit-id' section is expanded, showing 'Active' as unchecked, 'identifier-string' as empty, 'option' as 'spv', and 'delimiter' as '/'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Click **Port** on the top of the screen.

- 2 Select **Trusted** for ports 11 and 12 and then click **Apply**.

Port	Server Trusted State	Circuit-id	Remote-id
*	Untrusted		
1	Untrusted		
2	Untrusted		
3	Untrusted		
4	Untrusted		
5	Untrusted		
6	Untrusted		
7	Untrusted		
8	Untrusted		
9	Untrusted		
10	Untrusted		
11	Trusted		
12	Trusted		
13	Untrusted		
14	Untrusted		

Then Click **Intermediate Agent** on the top of the screen.

- 3 The **Intermediate Agent** screen appears. Click **VLAN** on the top of the screen.

Intermediate Agent | Port | **VLAN** | PPPoE

Active ☒

access-node-identifier XGS-4728F

circuit-id

Active ☐

identifier-string

option spv

delimiter /

Apply Cancel

- 4 Enter 1 for both **Start VID** and **End VID**. Click **Apply**.

VLAN Intermediate Agent

Show VLAN Start VID 1 End VID 1

Apply

VID	Enabled	Circuit-id	Remote-id
*	No	☐	☐

Apply Cancel

- 5 Then select **Yes** to enable PPPoE IA in VLAN 1 and also select **Circuit-id** and **Remote-id** to allow the Switch to add these two strings to frames tagged with VLAN 1 and pass to the PPPoE server. Click **Apply**.

VLAN Intermediate Agent

Show VLAN Start VID End VID

Apply

VID	Enabled	Circuit-id	Remote-id
*	No	☐	☐
1	Yes	☒	☒

Apply Cancel

The settings are completed now. If you miss some settings above, subscriber **C** could not successfully receive an IP address assigned by the PPPoE Server. If this happens, make sure you follow the steps exactly in this tutorial.

6.4 How to Use Error Disable and Recovery on the Switch

This tutorial shows you how to shut down a port when:

- there is a loop occurred

or

- too many ARP requests (over 100 packets per second) received on a port

You also want the Switch to wait for a period of time (10 minutes) before resuming the port automatically, after the problem(s) are gone. Loop guard and Errdiable features are helpful for this demand.

Note: Refer to [Section 27.2 on page 285](#) and [Section 32.3 on page 310](#) for more information about Loop Guard and Errdiable.

To configure the settings:

- 1 First, click **Advanced Application > Loop Guard**. Select the **Active** option in the first section to enable loop guard on the Switch. Then select the **Active** option of the first entry (port *) to enable loop guard for all ports. Click **Apply**.

Port	Active
*	☒
1	☒
2	☒
3	☒
4	☒
5	☒
6	☒
7	☒
8	☒
9	☒
10	☒
11	☒
12	☒

- 2 Click **Advanced Application > Errdisable > CPU Protection**, select **ARP** as the reason, enter 100 as the rate limit (packets per second) for the first entry (port *) to apply the setting to all ports. Then click **Apply**.

CPU protection Errdisable

Reason: **ARP** ▼

Port	Rate Limit (pkt/s)
*	100
1	100
2	100
3	100
4	100
5	100
6	100
7	100
8	100
9	100
10	100
11	100
12	100
13	100

- 3 Click **Advanced Application > Errdisable > Errdisable Detect**, select **Active** for cause **ARP** and **inactive-port** as the mode. Then click **Apply**.

Errdisable Detect Errdisable

Cause	Active	Mode
*	☐	inactive-port ▼
ARP	☒	inactive-port ▼
BPDU	☐	inactive-port ▼
IGMP	☐	inactive-port ▼

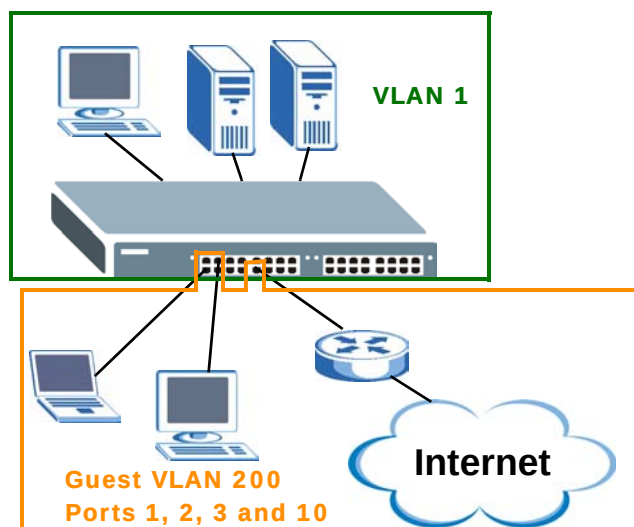
- 4 Click **Advanced Application > Errdisable > Errdisable Recovery**, select **Active** and **Timer Status** for **loopguard** and **ARP** entries. Also enter 180 (180 seconds = 3 minutes) in the **Interval** field for both entries. Then click **Apply**.

Reason	Timer Status	Interval
*	☐	
loopguard	☒	180
ARP	☒	180
BPDU	☐	300
IGMP	☐	300

Buttons: Apply, Cancel

6.5 How to Set Up a Guest VLAN

All ports on the Switch are in VLAN 1 by default. Say you enable IEEE 802.1x authentication on ports 1 to 8. Clients that connect to these ports should provide the correct user name and password in order to access the ports. You want to assign clients that connect to ports 1, 2 or 3 to a guest VLAN (200 for example) before they can authenticate with the authentication server. In this guest VLAN, clients can surf the Internet through the default gateway attached to port 10, but are not allowed to access other network resources, such as the mail server or local data base.



6.5.1 Creating a Guest VLAN

Follow the steps below to configure port 1, 2, 3 and 10 as a member of VLAN 200.

- 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.

Switch Setup

VLAN Type
☒ 802.1Q
☐ PortBased

Bridge Control Protocol Transparency Active ☐

MAC Address Learning
 Aging Time: 300 seconds
 Join Timer: 200 milliseconds
 Leave Timer: 600 milliseconds
 Leave All Timer: 10000 milliseconds

GARP Timer

Priority Queue Assignment

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

Apply Cancel

- 3 Click **Advanced Application > VLAN > Static VLAN**.
- 4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 200 for example) in the **Name** field and enter 200 in the **VLAN Group ID** field.
- 5 Select **Fixed** to configure ports 1, 2, 3 and 10 to be permanent members of this VLAN.
- 6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending frames out of these ports.

- 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.

Static VLAN VLAN Status

ACTIVE ☒

Name: VLAN 200

VLAN Group ID: 200

Port	Control			Tagging
*		Normal		☒ Tx Tagging
1	☐ Normal	☒ Fixed	☐ Forbidden	☐ Tx Tagging
2	☐ Normal	☒ Fixed	☐ Forbidden	☐ Tx Tagging
3	☐ Normal	☒ Fixed	☐ Forbidden	☐ Tx Tagging
4	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
5	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
6	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
7	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
8	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
9	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging
10	☐ Normal	☒ Fixed	☐ Forbidden	☐ Tx Tagging
11	☒ Normal	☐ Fixed	☐ Forbidden	☒ Tx Tagging

Add Cancel Clear

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

VLAN Status VLAN Port Setting Static VLAN

VLAN Search by VID: Search

The Number of VLAN: 4.

Index	VID	Elapsed Time	Status
1	1	2:59:05	Static
2	102	2:59:05	Static
3	123	2:59:05	Static
4	200	0:00:07	Static

Change Pages Previous Next

- 9 Enter 200 in the **PVID** field for ports 1, 2, 3 and 10 to add a tag to incoming untagged frames received on these ports so that the frames are forwarded to the VLAN group that the tag defines.

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

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	200	☐	All	☐	☐
2	☐	200	☐	All	☐	☐
3	☐	200	☐	All	☐	☐
4	☐	1	☐	All	☐	☐
5	☐	1	☐	All	☐	☐
6	☐	1	☐	All	☐	☐
7	☐	1	☐	All	☐	☐
8	☐	1	☐	All	☐	☐
9	☐	1	☐	All	☐	☐
10	☐	200	☐	All	☐	☐
11	☐	1	☐	All	☐	☐

Apply Cancel

- 11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

6.5.2 Enabling IEEE 802.1x Port Authentication

Follow the steps below to enable port authentication to validate access to ports 1~8 to clients based on a RADIUS server.

- 1 Click **Advanced Application > Port Authentication** and then the **Click Here** link for **802.1x**.

Port Authentication

802.1x	Click here
MAC Authentication	Click here

- 2 Select the first **Active** checkbox to enable 802.1x authentication on the Switch.

Select the **Active** checkboxes for ports 1 to 8 to turn on 802.1x authentication on the selected ports.

Click **Apply**.

802.1x Port Authentication **Guest Vlan**

Active ☒

Port	Active	Max-Req	Reauth	Reauth-period secs	Quiet-period secs	Tx-period secs	Supp-Timeout secs
*	☐		On ▼				
1	☒	2	On ▼	3600	60	30	30
2	☒	2	On ▼	3600	60	30	30
3	☒	2	On ▼	3600	60	30	30
4	☒	2	On ▼	3600	60	30	30
5	☒	2	On ▼	3600	60	30	30
6	☒	2	On ▼	3600	60	30	30
7	☒	2	On ▼	3600	60	30	30
8	☒	2	On ▼	3600	60	30	30
9	☐	2	On ▼	3600	60	30	30
10	☐	2	On ▼	3600	60	30	30

Apply Cancel

6.5.3 Enabling Guest VLAN

- 1 Click the **Guest Vlan** link in the **802.1x** screen.

- 2 Select **Active** and enter the guest VLAN ID (200 in this example) on ports 1, 2 and 3. The Switch puts unauthenticated clients in the specified guest VLAN.

Set **Host-mode** to **Multi-Secure** to have the Switch authenticate each client that connects to one of these ports, and specify the maximum number of clients that the Switch will authenticate on each of these port (5 in this example).

Click **Apply**.

Port	Active	Guest Vlan	Host-mode	Multi-Secure Num
*	☐		Multi-Host	
1	☒	200	Multi-Secure	5
2	☒	200	Multi-Secure	5
3	☒	200	Multi-Secure	5
4	☐	1	Multi-Host	1
5	☐	1	Multi-Host	1
6	☐	1	Multi-Host	1
7	☐	1	Multi-Host	1
8	☐	1	Multi-Host	1
9	☐	1	Multi-Host	1
28	☐	1	Multi-Host	1

Apply Cancel

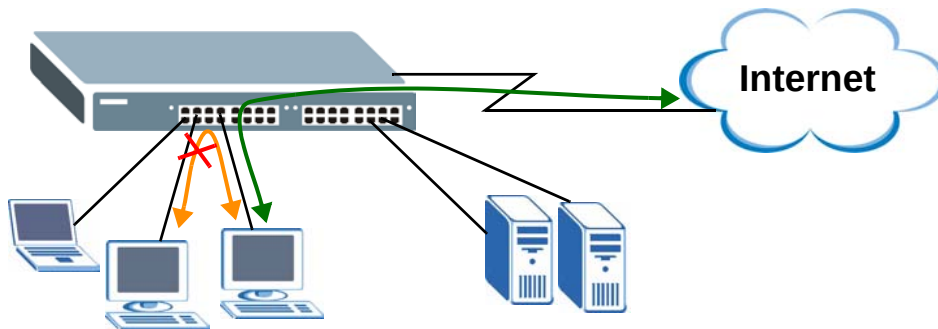
- 3 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

Clients that attach to port 1, 2 or 3 and fail to authenticate with the RADIUS server now should be in VLAN 200 and can access the Internet, but cannot communicate with devices in VLAN 1.

6.6 How to Do Port Isolation in a VLAN

You want to prevent communications between specific ports in a VLAN but still allow them to access the Internet or network resources in the same VLAN. You use

Private VLAN to do port isolation in a VLAN instead of assigning each port to a separate VLAN and creating a different IP routing domain for each individual port.



In this example, you put ports 2 to 5 in VLAN 123 and create a private VLAN rule for VLAN 123 to block traffic between ports 2, 3 and 4.

6.6.1 Creating a VLAN

Follow the steps below to configure port 2, 3, 4 and 5 as a member of VLAN 123.

- 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.

Switch Setup	
VLAN Type	☒ 802.1Q ☐ Port Based
Bridge Control Protocol Transparency	Active ☐
MAC Address Learning	Aging Time: 300 seconds Join Timer: 200 milliseconds Leave Timer: 600 milliseconds Leave All Timer: 10000 milliseconds
GARP Timer	
Priority Queue Assignment	level7: 7 level6: 6 level5: 5 level4: 4 level3: 3 level2: 1 level1: 0 level0: 2
Apply Cancel	

- 3 Click **Advanced Application > VLAN > Static VLAN**.

- 4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 123 for example) in the **Name** field and enter 123 in the **VLAN Group ID** field.
- 5 Select **Fixed** to configure ports 2, 3, 4 and 5 to be permanent members of this VLAN.
- 6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending frames out of these ports.
- 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.

Static VLAN VLAN Status

ACTIVE ☒

Name: VLAN 123

VLAN Group ID: 123

Port	Control	Tagging
*	Normal	☒ Tx Tagging
1	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
2	☐ Normal ☒ Fixed ☐ Forbidden	☐ Tx Tagging
3	☐ Normal ☒ Fixed ☐ Forbidden	☐ Tx Tagging
4	☐ Normal ☒ Fixed ☐ Forbidden	☐ Tx Tagging
5	☐ Normal ☒ Fixed ☐ Forbidden	☐ Tx Tagging
6	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
7	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
8	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
9	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging

Add

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

VLAN Status

VLAN Port Setting

Static VLAN

VLAN Search by VID Search

The Number of VLAN: 3.

Index	VID	Elapsed Time	Status
1	1	5:19:47	Static
2	102	5:19:47	Static
3	123	0:05:28	Static

Change Pages Previous Next

- 9 Enter 123 in the **PVID** field for ports 2, 3, 4 and 5 to add a tag to incoming untagged frames received on these ports so that the frames are forwarded to the VLAN group that the tag defines.
- 10 Click **Apply** to save your changes back to the run-time memory.

VLAN Port Setting

Subnet Based Vlan Protocol Based Vlan VLAN Status

GVRP ☐

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	1	☐	All	☐	☐
2	☐	123	☐	All	☐	☐
3	☐	123	☐	All	☐	☐
4	☐	123	☐	All	☐	☐
5	☐	123	☐	All	☐	☐
6	☐	1	☐	All	☐	☐
7	☐	1	☐	All	☐	☐
8	☐	1	☐	All	☐	☐
9	☐	1	☐	All	☐	☐

Apply Cancel

- 11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

6.6.2 Creating a Private VLAN Rule

Follow the steps below to configure private VLAN for VLAN 123.

- 1 Click **Advanced Application > Private VLAN**.
- 2 In the **Private VLAN** screen, select **Active**.

Enter a descriptive name (PrivateVLAN123 for example) in the **Name** field and enter 123 in the **VLAN ID** field.

List the port(s) that can communicate with any port in VLAN 123 (5 in this example). Then other ports in this VLAN (2, 3 and 4 for example) will be added to the isolated port list and cannot send traffic to each other.

Click **Add**.

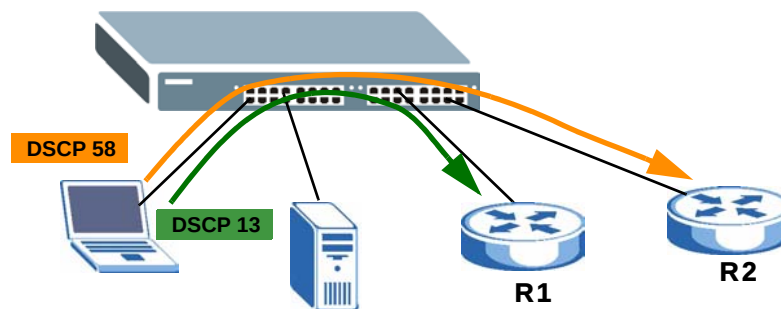
Private VLAN					
Active	☒				
Name	PrivateVLAN123				
VLAN ID	123				
Promiscuous Ports	5				
Add Cancel Clear					
Index	Active	Name	VLAN	Promiscuous Ports	Delete
Delete Cancel					

- 3 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

From port 2, 3, or 4, you should be able to access the device that attaches to port 5, such as a server or default gateway.

6.7 How to Configure Routing Policy

The Switch checks the routing table and then forwards traffic through the default gateway (**R1**) based on the destination address. This example shows you how to configure policy route to send traffic that matches a layer-3 classifier to a different gateway (**R2**) for special treatment. The layer-3 classifier groups packets marked with DSCP value 58 into a flow. Packets marked with different DSCP values, such as 13 are forwarded to the default gateway. The Switch applies policy-based routing rules to incoming packets prior to the normal routing.



6.7.1 Create a Layer-3 Classifier

Follow the steps below to configure a classifier that sorts traffic with DSCP value 58 into a data flow.

- 1 Access the web configurator through the Switch's management port.
- 2 Go to **Advanced Application > Classifier** and select **Active**.
Enter a descriptive name ("DSCP58" in this example).
Select the second option of **DSCP** and enter 58 in the field provided.

- 3 Click **Add** to save the settings to the run-time memory.

Classifier

Active ☒

Name DSCP58

Packet Format All

Layer 2

VLAN ☒ Any

Priority ☒ Any ☐ 0

Ethernet Type ☒ All ☐ Others (Hex)

Source MAC Address ☒ Any ☐ MAC

Port ☒ Any ☐ Port

Destination MAC Address ☒ Any ☐ MAC

Layer 3

DSCP ☐ Any ☒ 58

IP Protocol ☒ All ☐ Others (Dec) ☐ Establish Only

Source IP Address / Address Prefix 0.0.0.0 /

Socket Number ☒ Any ☐ Socket Number

Destination IP Address / Address Prefix 0.0.0.0 /

Socket Number ☒ Any ☐ Socket Number

Add Cancel Clear

6.7.2 Create a Policy Routing Rule

Follow the steps below to set up a policy routing profile first and then a rule to forward traffic of classifier **DSCP58** to gateway **R2**.

- 1 Click **IP Application > Policy Routing**.
- 2 Select **Active** and enter a descriptive name for this profile ("To_R2" for example). Click **Add** to save the settings to the run-time memory.

- 3 Click the **Rule Configuration** link in the **Policy Route** screen to create a rule in this profile.

Policy Route Rule Configuration

Active ☒

Profile Name

Add Cancel Clear

Index	Active	Profile name	Delete

Delete Cancel

- 4 Select the name of the profile with which the rule associates.
Set the rule's index number to 1 in the **Sequence** field.
Select **Permit** to have the Switch send matched traffic to the specified gateway.
Select the name of the layer-3 classifier to which the rule applies.
Enter the IP address of gateway **R2** in the **Next Hop** field ("10.1.2.3" in this example).
Click **Add** to save the settings to the run-time memory.

Policy Route Profile Configuration

Profile Name

Sequence

Statement ☒ Permit ☐ Deny

Classifier

Action

Add Cancel Clear

Active	Profile name	Seq	State	Classifier	Rule Delete
Yes	To_R2				

- 5 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

PART II

Technical Reference

System Status and Port Statistics

This chapter describes the system status (web configurator home page) and port details screens.

7.1 Overview

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

7.2 Port Status Summary

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

Figure 30 Status

Port Status										
Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
2	1000M/F Copper	FORWARDING	Disabled		0	108	0	0.0	0.0	0:47:09
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
13		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

☒ Any
 ☐ Port

The following table describes the labels in this screen.

Table 8 Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the Port Details screen (refer to Figure 31 on page 97).
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, 1000M for 1000 Mbps, and 10G for 10 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. (See Section 13.1.3 on page 149 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
LACP	This field displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Type a port number, select Port and then click Clear Counter to erase the recorded statistical information for that port, or select Any to clear statistics for all ports.

7.2.1 Status: Port Details

Click a number in the **Port** column in the **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 31 Status: Port Details

Port Details		Port Status
Port Info	Port NO.	1
	Name	
	Link	100M/F Copper
	Status	FORWARDING
	LACP	Disabled
	TxPkts	752
	RxPkts	710
	Errors	3
	Tx KBs/s	44.31
	Rx KBs/s	6.779
	Up Time	0:01:50
TX Packet	Unicast	751
	Multicast	0
	Broadcast	1
	Pause	0
	Tagged	0
RX Packet	Unicast	557
	Multicast	9
	Broadcast	141
	Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	3
	Length	0
	Runt	0
Distribution	64	573
	65 to 127	153
	128 to 255	150
	256 to 511	121
	512 to 1023	182
	1024 to 1518	283
	Giant	0

The following table describes the labels in this screen.

Table 9 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 10Mbps, 100M for 100Mbps, 1000M for 1000 Mbps, and 10G for 10 Gbps) and the duplex (F for full duplex or H for half duplex). It also shows the cable type (Copper or Fiber).

Table 9 Status > Port Details (continued)

LABEL	DESCRIPTION
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 13.1.3 on page 149 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet	
The following fields display detailed information about packets transmitted.	
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet	
The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision	
The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.

Table 9 Status > Port Details (continued)

LABEL	DESCRIPTION
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	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. See Chapter 56 on page 463.

Basic Setting

This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.

8.1 Overview

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

8.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. You can check the firmware version number and monitor the Switch temperature, fan speeds and voltage in this screen.

Figure 32 Basic Setting > System Info

System Info					
System Name	XGS-4728F				
Product Model	XGS-4728F				
ZyNOS F/W Version	V4.00(BBC.0)b3_20101130 11/30/2010				
Ethernet Address	00:19:cb:6f:91:59				

Hardware Monitor					
Temperature Unit	C				
Temperature (C)	Current	MAX	MIN	Threshold	Status
BOARD	40.0	41.0	40.0	75.0	Normal
PHY	34.0	34.0	33.0	85.0	Normal
MAC	44.0	44.0	43.0	85.0	Normal
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	< 41	0	0	3100	Error
FAN2	4131	4169	4109	3100	Normal
FAN3	2811	2821	2783	3100	Normal
Voltage (V)	Current	MAX	MIN	Threshold	Status
1.2VIN	1.217	1.217	1.217	+/-6%	Normal
1.25VIN	1.248	1.248	1.248	+/-6%	Normal
1.8VIN	1.843	1.843	1.843	+/-6%	Normal
3.3VIN	3.360	3.360	3.360	+/-6%	Normal
12VIN	11.594	11.594	11.594	+/-10%	Normal

The following table describes the labels in this screen.

Table 10 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 model number of the Switch.
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.
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	BOARD , PHY , and MAC refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.

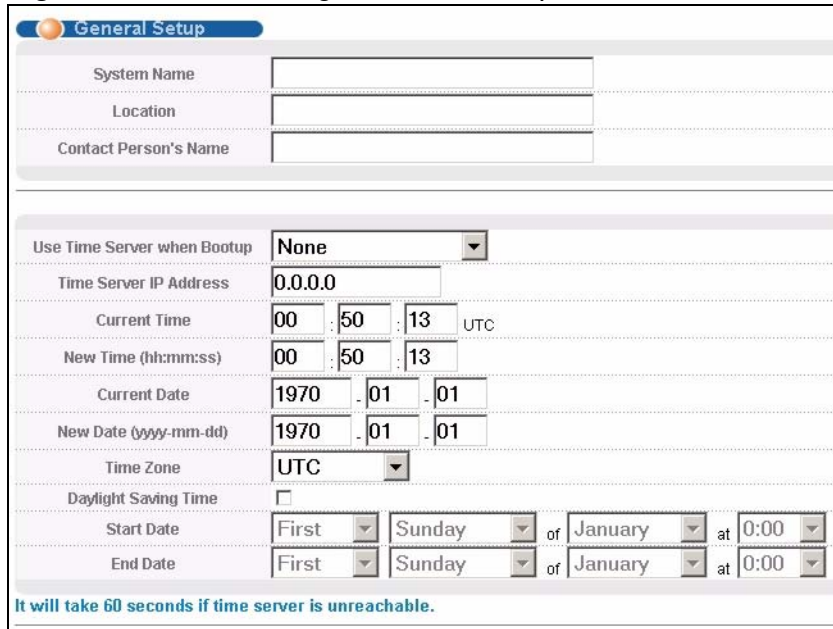
Table 10 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in RPM.
MIN	This field displays this fan's minimum speed measured in RPM. "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
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** and **General Setup** in the navigation panel to display the screen as shown.

Figure 33 Basic Setting > General Setup



The following table describes the labels in this screen.

Table 11 Basic Setting > General Setup

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

Table 11 Basic Setting > General Setup (continued)

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

Table 11 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
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 group(s); the traffic must first go through a router.

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

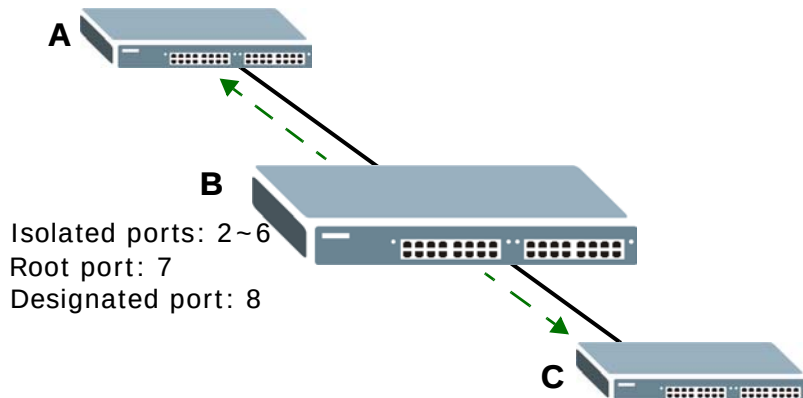
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

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

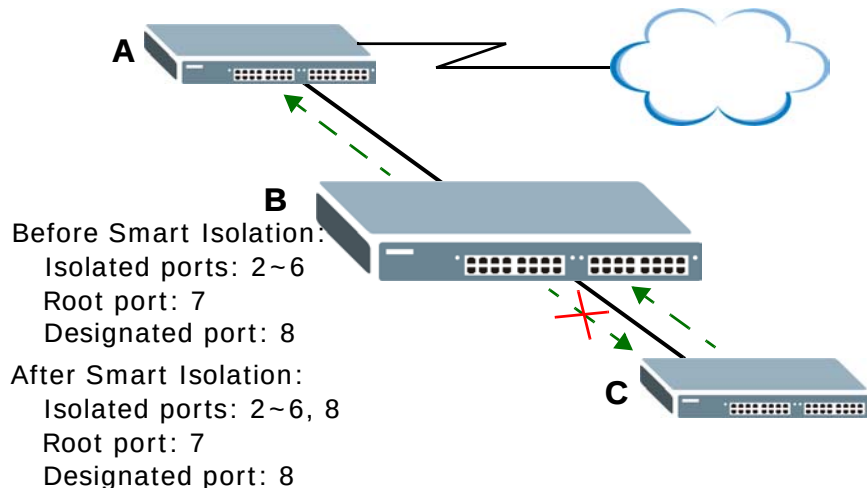
See [Chapter 9 on page 117](#) for information on port-based and 802.1Q tagged VLANs.

8.4.1 Smart Isolation

To block traffic between two specific ports within the Switch, you can use port isolation or private VLAN (see [Chapter 33 on page 315](#) for more information). However, it does not work across multiple switches. For example, broadcast traffic from isolated ports on a switch (say **B**) can be forwarded to all ports on other switches (**A** and **C**), including the isolated ports.



Smart isolation allows you to prevent isolated ports on different switches from transmitting traffic to each other. After you enable RSTP/MRSTP and smart isolation on the Switch, the designated port(s) will be added to the isolated port list. In the following example, switch **A** is the root bridge. Switch **B**'s root port **7** connects to switch **A** and switch **B**'s designated port **8** connects to switch **C**. Traffic from isolated ports on switch **B** can only be sent through non-isolated port **1** or root port **7** to switch **A**. This prevents isolated ports on switch **B** sending traffic through designated port **8** to switch **C**. Traffic received on designated port **8** from switch **C** will not be forwarded to any other isolated ports on switch **B**.



You should enable RSTP or MRSTP before you can use smart isolation on the Switch. If the network topology changes, the Switch automatically updates the isolated port list with the latest designated port information.

Note: The uplink port connected to the Internet should be the root port. Otherwise, with smart isolation enabled, the isolated ports cannot access the Internet.

8.5 Switch Setup Screen

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

Figure 34 Basic Setting > Switch Setup

The following table describes the labels in this screen.

Table 12 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. See Chapter 9 on page 117 for more information.
Bridge Control Protocol Transparency	Select Active to allow the Switch to handle bridging control protocols (STP, for example). You also need to define how to treat a BPDU in the Port Setup screen.

Table 12 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
Smart Isolation	Select Active to enable smart isolation on the Switch. The designated port(s) then becomes the isolated port. Smart isolation allows you to prevent isolated ports on different switches from transmitting traffic to each other. Note: To use smart isolation, you should have configured 802.1Q VLAN port isolation or private VLAN and (M)RSTP on the Switch. Smart isolation does not work with MSTP and/or port-based VLAN.
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).
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See Chapter 9 on page 117 for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See Chapter 9 on page 117 for more background information.
Leave Timer	Leave Time sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer ; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the following fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested. Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.

Table 12 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click Apply to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

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 Interfaces

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

On the Switch, as a layer-3 device, an IP address is not bound to any physical ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the

Switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

Figure 35 Basic Setting > IP Setup

IP Setup

Default Gateway: 0.0.0.0

Domain Name Server: 0.0.0.0

Default Management: ☒ In-band ☐ Out-of-band

Management IP Address

IP Address: 192.168.0.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply Cancel

IP Interface

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

VID:

Add Cancel

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.12	255.255.255.0	1	☐

Delete Cancel

The following table describes the labels in this screen.

Table 13 Basic Setting > IP Setup

LABEL	DESCRIPTION
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow (In-Band or Out-of-band) the Switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source. Select Out-of-band to have the Switch send the packets to the management port labelled MGMT. This means that device(s) connected to the other port(s) do not receive these packets. Select In-Band to have the Switch send the packets to all ports except the management port (labelled MGMT) to which connected device(s) do not receive these packets.
Management IP Address	
Use these fields to set the settings for the out-of-band management port.	

Table 13 Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
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.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.0.254
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
IP Interface	
Use these fields to create or edit IP routing domains on the Switch.	
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 192.168.1.1. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click 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.
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.
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 Delete check boxes.

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 36 Basic Setting > Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control	CX4 Cable
*	☐		-	Auto	☐	0	Peer	0.5m
1	☒		10/100/1000M	Auto	☐	0	Peer	-
2	☒		10/100/1000M	Auto	☐	0	Peer	-
3	☒		10/100/1000M	Auto	☐	0	Peer	-
25	☒		10G	10G / Full Duplex	☐	0	Peer	-
26	☒		10G	10G / Full Duplex	☐	0	Peer	-
27	☒		10G/12G	12G / Full Duplex	☐	0	Peer	0.5m
28	☒		10G/12G	12G / Full Duplex	☐	0	Peer	0.5m

Apply Cancel

The following table describes the labels in this screen.

Table 14 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	Type a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitations, the port name may be truncated in some web configurator screens.
Type	This field displays 10/100/1000M for a 1000Base-T connection, 10G for a 10 Gigabit Ethernet connection, and 12G for a 10GBase-CX4 connection in the XGS-4528F or XGS-4728F.

Table 14 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Speed/ Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. The choices are Auto, 10M / Half Duplex, 10M / Full Duplex, 100M / Half Duplex and 100M / Full Duplex for a 1000Base-T connection. 1000M / Full Duplex is supported by both 1000Base-T and 1000Base-X connections. 10G / Full Duplex is supported by the 10 Gigabit Ethernet connections. 12G / Full Duplex is supported by the 10GBase-CX4 connections in the XGS-4528F or XGS-4728F. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 12 on page 108 for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch Setup screen first. Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port. Select Tunnel to forward BPDUs received on this port. Select Discard to drop any BPDU received on this port. Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.
CX4 Cable	For the XGS-4526, this field is available when you install an EM-412 module in the Switch's optional uplink module slot (see Section 3.2 on page 41). Select the number of meters for the length of the 10GBASE-CX4 cable you use to connect between the Switch and another switch for stacking.

Table 14 Basic Setting > Port 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.

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

9.1 Introduction to IEEE 802.1Q Tagged VLANs

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

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

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

9.1.1 Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware

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

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

9.2 Automatic VLAN Registration

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

9.2.1 GARP

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

9.2.1.1 GARP Timers

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

9.2.2 GVRP

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

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

Table 15 IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.

Table 15 IEEE 802.1Q VLAN Terminology (continued)

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member.

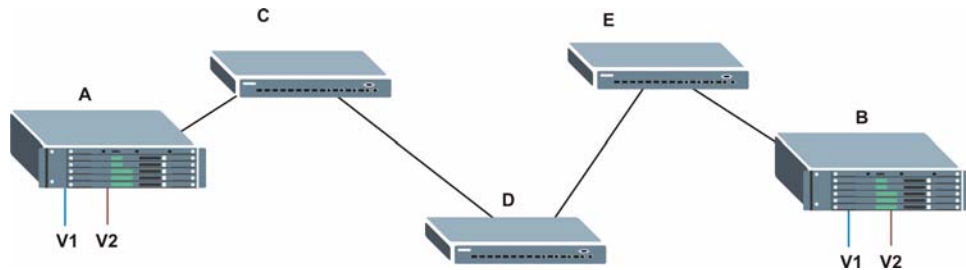
9.3 Port VLAN Trunking

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

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

allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

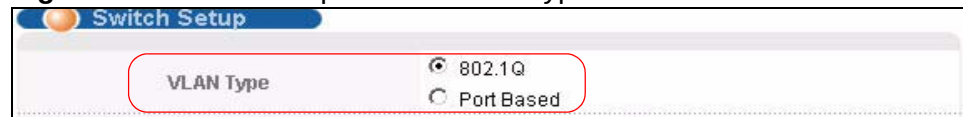
Figure 37 Port VLAN Trunking



9.4 Select the VLAN Type

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

Figure 38 Switch Setup: Select VLAN Type



9.5 Static VLAN

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

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

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

9.5.1 VLAN Status

See [Section 9.1 on page 117](#) for more information on Static VLAN. Click **Advanced Application > VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 39 Advanced Application > VLAN: VLAN Status

Index	VID	Elapsed Time	Status
1	1	0:52:21	Static

The following table describes the labels in this screen.

Table 16 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click Search to display only the specified VLAN(s) in the list below. Leave this field blank and click Search to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the Search button to look for certain VLANs.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch; dynamic - using GVRP, static - added as a permanent entry or other - added in another way such as via Multicast VLAN Registration (MVR).
Change Pages	Click Previous or Next to show the previous/next screen if all status information cannot be seen in one screen.

9.5.2 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See [Section 9.1 on page 117](#) for more information on static VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 40 Advanced Application > VLAN > VLAN Detail

VID	Port Number														Elapsed Time	Status
	2	4	6	8	10	12	14	16	18	20	22	24	26	28		
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	3:22:07	Static

The following table describes the labels in this screen.

Table 17 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the VLAN Status screen.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
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 or other - added in another way such as via Multicast VLAN Registration (MVR).

9.5.3 Configure a Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the Switch. See [Section 9.1 on page 117](#) for more information on static VLAN. To configure a

static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 41 Advanced Application > VLAN > Static VLAN

Static VLAN VLAN Status

ACTIVE ☐

Name

VLAN Group ID

Port	Control	Tagging
*	Normal	☒ Tx Tagging
1	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
2	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
3	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
4	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
5	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
6	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
7	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging
8	☒ Normal ☐ Fixed ☐ Forbidden	☒ Tx Tagging

Add Cancel Clear

VID	Active	Name	Delete
1	Yes	1	☐

Delete Cancel

The following table describes the related labels in this screen.

Table 18 Advanced Application > VLAN > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters; 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.

Table 18 Advanced Application > VLAN > Static VLAN (continued)

LABEL	DESCRIPTION
Control	Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select Fixed for the port to be a permanent member of this VLAN group. Select Forbidden if you want to prohibit the port from joining this VLAN group.
Tagging	Select TX Tagging if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click 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.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

9.5.4 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See [Section 9.1 on page 117](#) for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 42 Advanced Application > VLAN > VLAN Port Setting

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	1	☐	All	☐	☐
2	☐	1	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐
5	☐	1	☐	All	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 19 Advanced Application > VLAN > VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All, Tag Only and Untag Only. Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped.
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 allow 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.

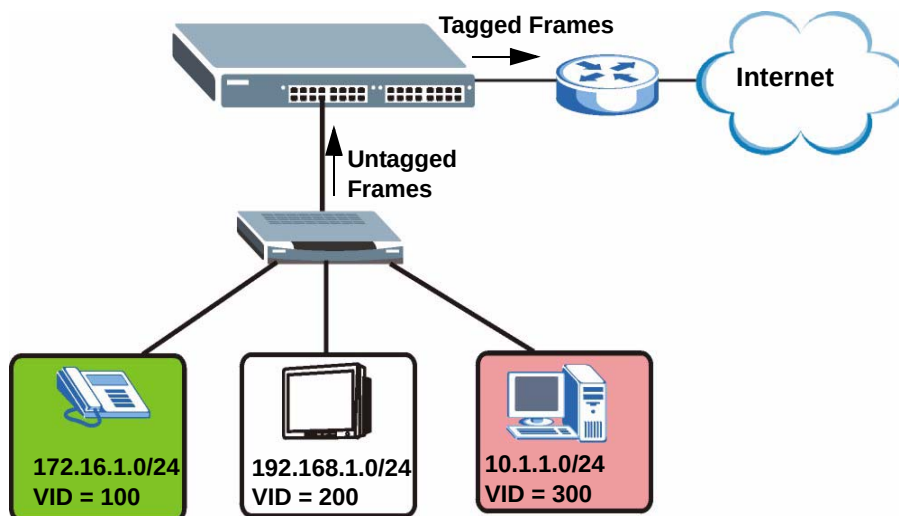
9.6 Subnet Based VLANs

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

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

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

Figure 43 Subnet Based VLAN Application Example



9.7 Configuring Subnet Based VLAN

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

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

Figure 44 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN

The following table describes the labels in this screen.

Table 20 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click 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 alphanumeric characters to identify this subnet based VLAN.

Table 20 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup (continued)

LABEL	DESCRIPTION
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 Applications > VLAN screens.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click Cancel to begin configuring this screen afresh.

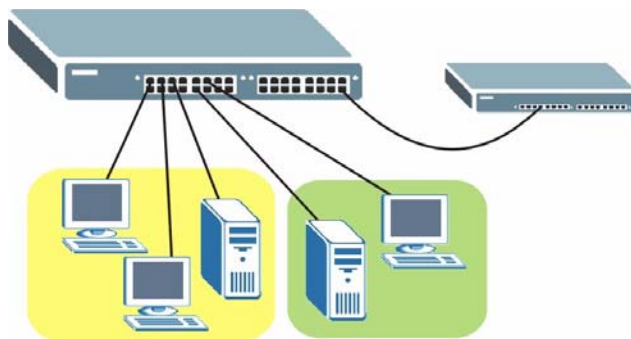
9.8 Protocol Based VLANs

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, ports 1, 2, 3 and 4 belong to static VLAN 100, and ports 4, 5, 6, 7 belong to static VLAN 120. You can configure a protocol based VLAN A with priority 3 for ARP traffic received on port 1, 2 and 3. You can 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 45 Protocol Based VLAN Application Example



9.9 Configuring Protocol Based VLAN

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

Figure 46 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN

Protocol Based VLAN

Vlan Port Setting

Active

☐

Port

Name

Ethernet-type

☒ IP
 ☐ Others (Hex)

VID

Priority

Add

Cancel

Index	Active	Port	Name	Ethernet-type	VID	Priority	Delete
Delete Cancel							

The following table describes the labels in this screen.

Table 21 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this protocol based VLAN.
Port	Type a port number to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 9 on page 117 for more details on setting up VLANs.
Name	Enter up to 32 alphanumeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select Others and type the protocol number in hexadecimal notation. For example, the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the Advanced Applications > VLAN screens.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name the protocol based VLAN.
Ethernet-type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click Cancel to begin configuring this screen afresh.

9.10 Create an IP-based VLAN Example

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

- 1 Activate this protocol based VLAN.
- 2 Type the port number you want to include in this protocol based VLAN. Type **1**.
- 3 Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.
- 4 Select the protocol. Leave the default value **IP**.
- 5 Type the VLAN ID of an existing VLAN. In our example we already created a static VLAN with an ID of 5. Type **5**.
- 6 Leave the priority set to **0** and click **Add**.

Figure 47 Protocol Based VLAN Configuration Example

Protocol Based VLAN

Active ☒

Port

Name

Ethernet-type ☒ IP ☐ Others (Hex)

VID

Priority

Add Cancel

Index	Active	Port	Name	Ethernet-type	VID	Priority	Delete

Delete Cancel

EXAMPLE

To add more ports to this protocol based VLAN.

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

9.11 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.

9.11.1 Configure a Port-based VLAN

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

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

Figure 48 Advanced Application > VLAN > Port Based VLAN Setup (All Connected)

Port Based VLAN Setup

Setting Wizard All connected ▾ Apply

Incoming

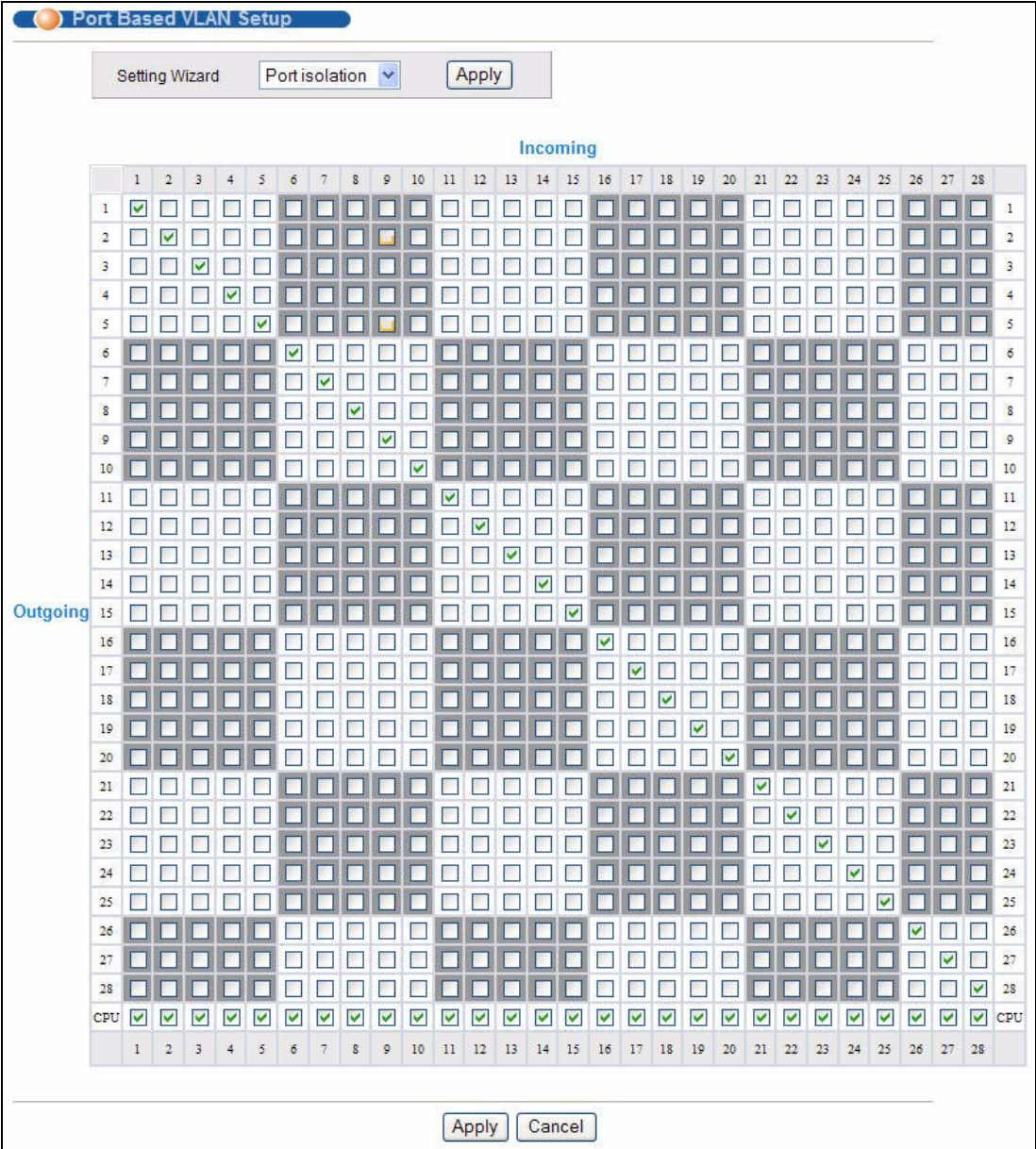
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1
2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2
3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	3
4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	4
5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	5
6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	6
7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	7
8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	8
9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	9
10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10
11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	11
12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	12
13	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	13
14	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
15	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	15
16	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	16
17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17
18	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	18
19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	19
20	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	20
21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21
22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	22
23	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	23
24	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	24
25	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	25
26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	26
27	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	27
28	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	28
CPU	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	CPU

Outgoing

Apply Cancel

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

Figure 49 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 22 Advanced Application > VLAN: Port Based VLAN Setup

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

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

10.1 Overview

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

10.2 Configuring Static MAC Forwarding

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

Static MAC address forwarding together with port security allows only computers in the MAC address table on a port to access the Switch. See [Chapter 19 on page 197](#) for more information on port security.

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

Figure 50 Advanced Application > Static MAC Forwarding

The following table describes the labels in this screen.

Table 23 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 Add to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.

Table 23 Advanced Application > Static MAC Forwarding (continued)

LABEL	DESCRIPTION
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

Static Multicast Forward Setup

Use these screens to configure static multicast address forwarding.

11.1 Static Multicast Forwarding Overview

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

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. You can configure this in the **Advanced Application > Multicast > Multicast Setting** screen (see [Section 24.3 on page 229](#)). [Figure 51](#) shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. [Figure 52](#) shows frames being forwarded to devices

connected to port 3. [Figure 53](#) shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 51 No Static Multicast Forwarding

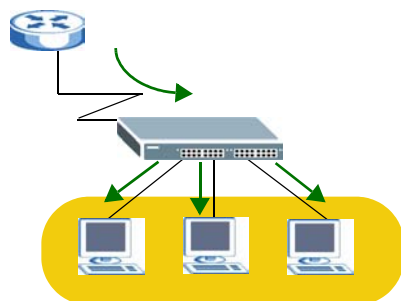


Figure 52 Static Multicast Forwarding to A Single Port

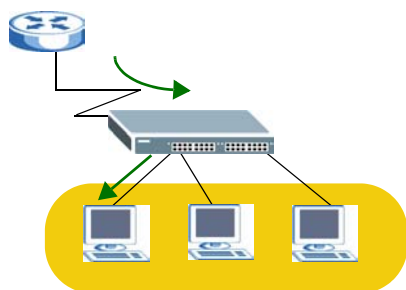
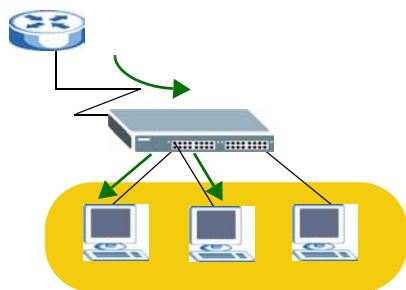


Figure 53 Static Multicast Forwarding to Multiple Ports



11.2 Configuring Static Multicast Forwarding

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

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

Figure 54 Advanced Application > Static Multicast Forwarding

The following table describes the labels in this screen.

Table 24 Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Add	Click Add to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the 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 port(s).

Table 24 Advanced Application > Static Multicast Forwarding (continued)

LABEL	DESCRIPTION
Active	This field displays whether a static multicast MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

Filtering

This chapter discusses MAC address port filtering.

12.1 Configure a Filtering Rule

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

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

Figure 55 Advanced Application > Filtering

The screenshot shows the 'Filtering' configuration interface. It includes a title bar, a form with fields for 'Active' (checkbox), 'Name' (text input), 'Action' (checkboxes for 'Discard source' and 'Discard destination'), 'MAC' (text input with colons), and 'VID' (text input). Below the form are 'Add', 'Cancel', and 'Clear' buttons. At the bottom is a table with columns: Index, Active, Name, MAC Address, VID, Action, and Delete. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the related labels in this screen.

Table 25 Advanced Application > Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.

Table 25 Advanced Application > Filtering (continued)

LABEL	DESCRIPTION
Action	Select Discard source to drop frames from the source MAC address (specified in the MAC field). The Switch can still send frames to the MAC address. Select Discard destination to drop frames to the destination MAC address (specified in the MAC address). The Switch can still receive frames originating from the MAC address. Select Discard source and Discard destination to block traffic to/from the MAC address specified in the MAC field.
MAC	Type a MAC address in a valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click 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 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 purposes only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es) in the Delete column.

Spanning Tree Protocol

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

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

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

13.1 STP/RSTP Overview

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

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

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

13.1.1 STP Terminology

The root bridge is the base of the spanning tree.

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

Table 26 STP Path Costs

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

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

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

13.1.2 How STP Works

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

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

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

13.1.3 STP Port States

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

Table 27 STP Port States

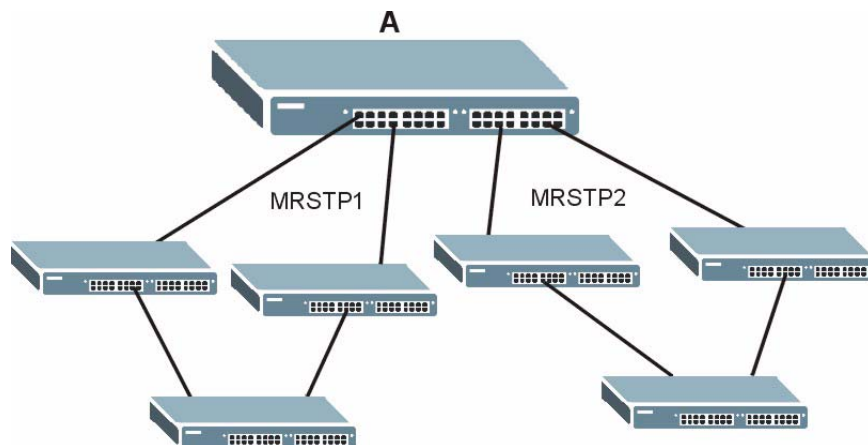
PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are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

13.1.4 Multiple RSTP

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

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

Figure 56 MRSTP Network Example



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

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

13.1.5 Multiple STP

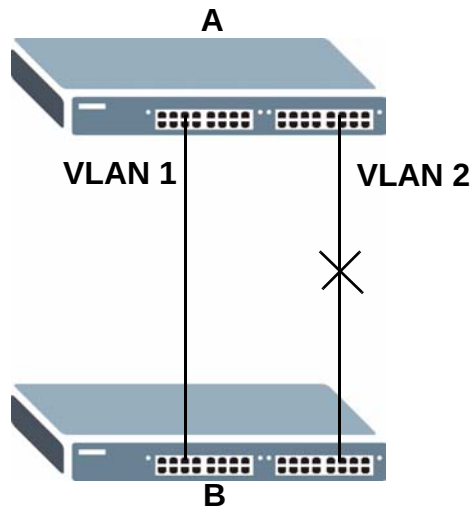
Multiple Spanning Tree Protocol (IEEE 802.1s) is backwards compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

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

13.1.5.1 MSTP Network Example

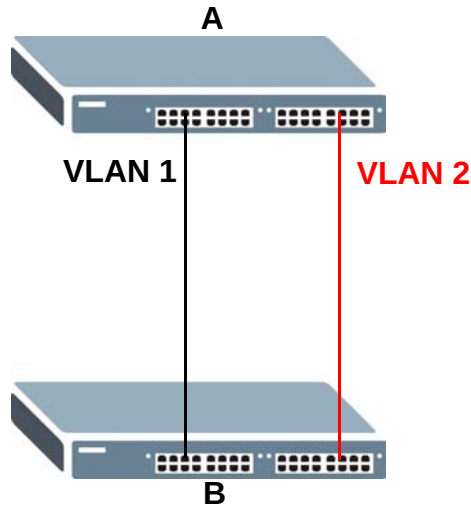
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 57 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 58 MSTP Network Example



13.1.5.2 MST Region

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

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

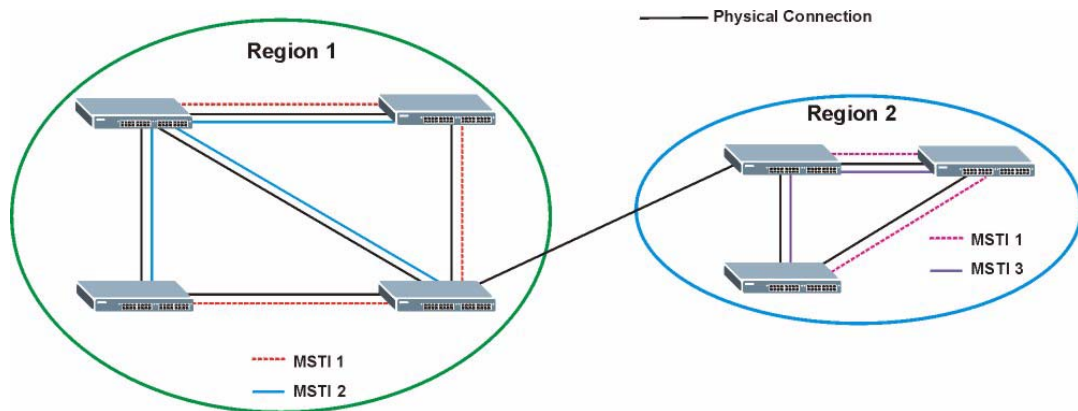
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

13.1.5.3 MST Instance

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

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

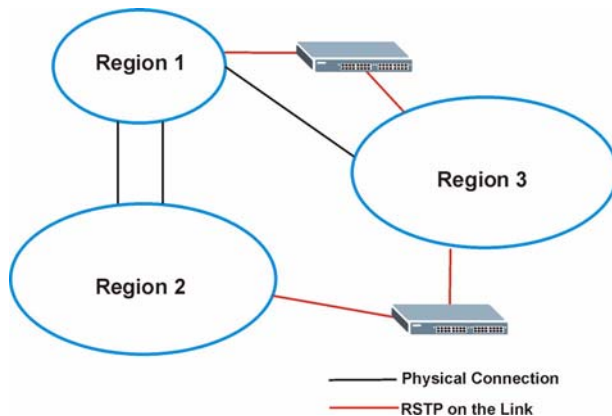
Figure 59 MSTIs in Different Regions



13.1.5.4 Common and Internal Spanning Tree (CIST)

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

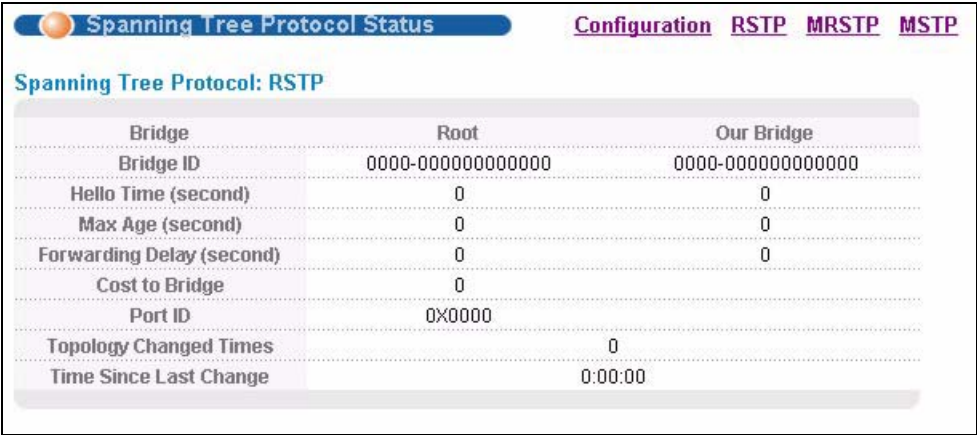
Figure 60 MSTP and Legacy RSTP Network Example



13.2 Spanning Tree Protocol Status Screen

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

Figure 61 Advanced Application > Spanning Tree Protocol



The screenshot shows the 'Spanning Tree Protocol Status' screen with tabs for Configuration, RSTP, MRSTP, and MSTP. The 'RSTP' tab is selected, displaying the following table:

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

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

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 62 Advanced Application > Spanning Tree Protocol > Configuration



The screenshot shows the 'Spanning Tree Configuration' screen with a 'Status' tab. Under 'Spanning Tree Mode', the following options are listed:

- ☒ Rapid Spanning Tree
- ☐ Multiple Rapid Spanning Tree
- ☐ Multiple Spanning Tree

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

The following table describes the labels in this screen.

Table 28 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select Rapid Spanning Tree , Multiple Rapid Spanning Tree or Multiple Spanning Tree . See Section 13.1 on page 147 for background information on STP.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 13.1 on page 147](#) for more information on RSTP. Click **RSTP** in the **Advanced Application > Spanning Tree Protocol** screen.

Figure 63 Advanced Application > Spanning Tree Protocol > RSTP

Rapid Spanning Tree Protocol Status

Active ☐

Bridge Priority 32768

Hello Time 2 Seconds

MAX Age 20 Seconds

Forwarding Delay 15 Seconds

Port	Active	Edge	Priority	Path Cost
*	☐	☐		
1	☐	☒	128	4
2	☐	☒	128	4
3	☐	☒	128	4
4	☐	☒	128	4
5	☐	☒	128	4
6	☐	☒	128	4
7	☐	☒	128	4
27	☐	☒	128	2
28	☐	☒	128	2

The following table describes the labels in this screen.

Table 29 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click Status to display the RSTP Status screen (see Figure 64 on page 157).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP. Note: You must also activate Rapid Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable RSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 29 Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
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).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 26 on page 148 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.

13.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 13.1 on page 147](#) for more information on RSTP.

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

Figure 64 Advanced Application > Spanning Tree Protocol > Status: RSTP

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

The following table describes the labels in this screen.

Table 30 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click RSTP to edit RSTP settings on the Switch.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of the bridge priority plus the MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). See Section 13.1.3 on page 149 for information on port states. Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

13.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 13.1 on page 147](#) for more information on MRSTP.

Figure 65 Advanced Application > Spanning Tree Protocol > MRSTP

Tree	Active	Bridge Priority	Hello Time	MAX Age	Forwarding Delay
1	☐	32768	2 seconds	20 seconds	15
2	☐	32768	2 seconds	20 seconds	15
3	☐	32768	2 seconds	20 seconds	15
4	☐	32768	2 seconds	20 seconds	15

Port	Active	Edge	Priority	Path Cost	Tree
*	☐	☐			1
1	☐	☒	128	4	1
2	☐	☒	128	4	1
3	☐	☒	128	4	1
4	☐	☒	128	4	1
5	☐	☒	128	4	1
27	☐	☒	128	2	1
28	☐	☒	128	2	1

Apply Cancel

The following table describes the labels in this screen.

Table 31 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click Status to display the MRSTP Status screen (see Figure 64 on page 157).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate Multiple Rapid Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable MRSTP on the Switch.

Table 31 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) 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: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).

Table 31 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

LABEL	DESCRIPTION
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the Switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended that you assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 26 on page 148 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.7 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 13.1 on page 147](#) for more information on MRSTP.

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

Figure 66 Advanced Application > Spanning Tree Protocol > Status: MRSTP

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

The following table describes the labels in this screen.

Table 32 Advanced Application > Spanning Tree Protocol > Status: MRSTP

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

13.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 13.1.5 on page 150](#) for more information on MSTP.

Figure 67 Advanced Application > Spanning Tree Protocol > MSTP

Multiple Spanning Tree Protocol

[Port](#)
[Status](#)

Bridge:

Active

☐

Hello Time

2

seconds

MAX Age

20

seconds

Forwarding Delay

15

seconds

Maximum hops

20

Configuration Name

0019cb6f9159

Revision Number

0

Apply

Cancel

Instance:

Instance

Bridge Priority

32768

VLAN Range

Start

End

Add

Remove

Clear

Enabled VLAN(s)

Port	Active	Priority	Path Cost
*	☐		
1	☐	128	4
2	☐	128	4
3	☐	128	4
4	☐	128	4
5	☐	128	4
6	☐	128	4
26	☐	128	2
27	☐	128	2
28	☐	128	2

Add

Cancel

Instance	VLAN	Active Port	Delete
0	1-4094	-	

Delete

Cancel

The following table describes the labels in this screen.

Table 33 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click Status to display the MSTP Status screen (see Figure 69 on page 166).
Active	Select this check box to activate MSTP on the Switch. Clear this checkbox to disable MSTP on the Switch. Note: You must also activate Multiple Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable MSTP on the Switch.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
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: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-16.

Table 33 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the Start field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the End field. Next click: • Add - to add this range of VLAN(s) to be mapped to the MST instance. • Remove - to remove this range of VLAN(s) from being mapped to the MST instance. • Clear - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
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 add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the Switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 26 on page 148 for more information.
Add	Click Add to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the 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.

Table 33 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to begin configuring this screen afresh.

13.8.1 Multiple Spanning Tree Protocol Port Configuration

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

Figure 68 Advanced Application > Spanning Tree Protocol > MSTP > Port

Port	Edge
*	☐
1	☒
2	☒
3	☒
4	☒
5	☒
6	☒
7	☒
8	☒
9	☒
10	☒
11	☒
12	☒
13	☒
28	☒

Apply Cancel

The following table describes the labels in this screen.

Table 34 Advanced Application > Spanning Tree Protocol > MSTP > 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.

Table 34 Advanced Application > Spanning Tree Protocol > MSTP > Port

LABEL	DESCRIPTION
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).
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 Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 13.1.5 on page 150](#) for more information on MSTP.

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

Figure 69 Advanced Application > Spanning Tree Protocol > Status: MSTP

Spanning Tree Protocol Status Configuration RSTP MRSTP MSTP

Spanning Tree Protocol: MSTP

CST

Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	8000-000000000000
Hello Time (second)	0	2
Max Age (second)	0	20
Forwarding Delay (second)	0	15
Cost to Bridge	0	0
Port ID	0x0000	0x0000
Configuration Name	001349000002	
Revision Number	0	
Configuration Digest	A317523DB32DA2D62	
Topology Changed Times	0	
Time Since Last Change	0	

Instance:

Instance	VLAN
0	1-4093

MSTI 1

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

The following table describes the labels in this screen.

Table 35 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click MSTP to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	Root refers to the base of the MST instance. Our Bridge is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.

Table 35 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
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.

Bandwidth Control

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

14.1 Bandwidth Control Overview

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

14.1.1 CIR and PIR

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

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

Note: The CIR should be less than the PIR.

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

14.2 Bandwidth Control Setup

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

Figure 70 Advanced Application > Bandwidth Control

Port	Active	Commit Rate	Ingress Rate Active	Peak Rate	Active	Egress Rate
*	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
1	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
2	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
3	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
4	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
5	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
6	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
7	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps
8	☐	1 Kbps	☐	1 Kbps	☐	1 Kbps

Apply Cancel

The following table describes the related labels in this screen.

Table 36 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.
Ingress Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.

Table 36 Advanced Application > Bandwidth Control (continued)

LABEL	DESCRIPTION
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Broadcast Storm Control

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

15.1 Broadcast Storm Control Setup

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

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

Figure 71 Advanced Application > Broadcast Storm Control

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
*	☐	☐	☐
1	☐ 0	☐ 0	☐ 0
2	☐ 0	☐ 0	☐ 0
3	☐ 0	☐ 0	☐ 0
4	☐ 0	☐ 0	☐ 0
5	☐ 0	☐ 0	☐ 0
6	☐ 0	☐ 0	☐ 0
7	☐ 0	☐ 0	☐ 0
8	☐ 0	☐ 0	☐ 0

Apply Cancel

The following table describes the labels in this screen.

Table 37 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 a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Mirroring

This chapter discusses port mirroring setup screens.

16.1 Port Mirroring Setup

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

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

Figure 72 Advanced Application > Mirroring

Port	Mirrored	Direction
*	☐	Ingress
1	☐	Ingress
2	☐	Ingress
3	☐	Ingress
4	☐	Ingress
5	☐	Ingress
6	☐	Ingress
7	☐	Ingress
8	☐	Ingress

The following table describes the labels in this screen.

Table 38 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Type the port number of the monitor port.
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 begin configuring this screen afresh.

Link Aggregation

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

17.1 Link Aggregation Overview

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

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

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

The Switch supports both static and dynamic link aggregation.

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

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

17.2 Dynamic Link Aggregation

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

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

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

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

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

17.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information¹:

Table 39 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 40 Link Aggregation ID: Peer Switch

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

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

17.3 Link Aggregation Status

Click **Advanced Application > Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See [Section 17.1 on page 177](#) for more information.

Figure 73 Advanced Application > Link Aggregation Status

Link Aggregation Status						Link Aggregation Setting
Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status	
T1	4	-	-	src-dst-mac	Static	
T2	5	-	[(0000,00-00-00-00-00-00,0000,00,0000)]	src-dst-mac	LACP	
T3	-	-	-	src-dst-mac	-	
T4	-	-	-	src-dst-mac	-	
T5	-	-	-	src-dst-mac	-	
T6	-	-	-	src-dst-mac	-	
T7	-	-	-	src-dst-mac	-	
T8	-	-	-	src-dst-mac	-	
T9	-	-	-	src-dst-mac	-	
T10	-	-	-	src-dst-mac	-	
T11	-	-	-	src-dst-mac	-	
T12	-	-	-	src-dst-mac	-	

The following table describes the labels in this screen.

Table 41 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Port	These are the ports you have configured in the Link Aggregation screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 17.2.1 on page 178 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.

Table 41 Advanced Application > Link Aggregation Status (continued)

LABEL	DESCRIPTION
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.

17.4 Link Aggregation Setting

Click **Advanced Application > Link Aggregation > Link Aggregation Setting** to display the screen shown next. See [Section 17.1 on page 177](#) for more information on link aggregation.

Figure 74 Advanced Application > Link Aggregation > Link Aggregation Setting

Group ID	Active	Criteria
T1	☒	src-dst-mac
T2	☒	src-dst-mac
T3	☐	src-dst-mac
T4	☐	src-dst-mac
T5	☐	src-dst-mac
T6	☐	src-dst-mac
T7	☐	src-dst-mac
T8	☐	src-dst-mac
T9	☐	src-dst-mac
T10	☐	src-dst-mac
T11	☐	src-dst-mac
T12	☐	src-dst-mac

Port	Group
1	None
2	None
3	None
4	T1
5	T2
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None
14	None
15	None
16	None
17	None
18	None
19	None
20	None
21	None
22	None
23	None
24	None
25	None
26	None
27	None
28	None

Apply Cancel

The following table describes the labels in this screen.

Table 42 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.

Table 42 Advanced Application > Link Aggregation > Link Aggregation Setting

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.

17.5 Link Aggregation Control Protocol

Click in the **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP** to display the screen shown next. See [Section 17.2 on page 177](#) for more information on dynamic link aggregation.

Figure 75 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

Link Aggregation Control Protocol

Link Aggregation Setting

Active

☒

System Priority

65535

Group ID	LACP Active
T1	☐
T2	☒
T3	☒
T4	☐
T5	☐
T6	☐
T7	☐
T8	☐
T9	☐
T10	☐
T11	☐
T12	☐

Port	LACP Timeout
*	30 seconds
1	30 seconds
2	30 seconds
3	30 seconds
4	30 seconds
5	30 seconds
6	30 seconds
7	30 seconds
8	30 seconds
28	30 seconds

Apply

Cancel

The following table describes the labels in this screen.

Table 43 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

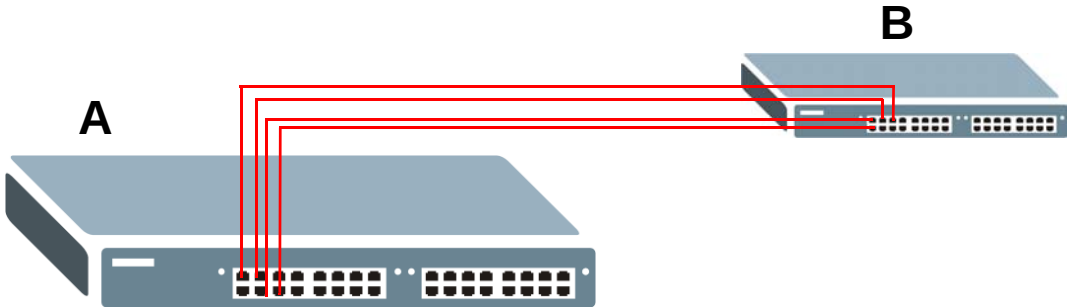
LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
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.

17.6 Static Trunking Example

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

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

Figure 76 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 77 Trunking Example - Configuration Screen

The screenshot shows the 'Link Aggregation Setting' configuration page. At the top, there's a header with 'Link Aggregation Setting' and 'Status LACP'. Below this is a table with columns 'Group ID', 'Active', and 'Criteria'. The table lists trunk groups T1 through T12. T1 is selected with a red circle around its row. In the 'Active' column, the checkbox for T1 is checked. In the 'Criteria' column, 'src-dst-mac' is selected. Below the table is a section for port assignment with columns 'Port' and 'Group'. Ports 2, 3, 4, and 5 are assigned to group T1, also highlighted with a red circle. At the bottom, there are 'Apply' and 'Cancel' buttons, with 'Apply' highlighted by a red circle. A red 'EXAMPLE' label is also present.

Group ID	Active	Criteria
T1	☒	src-dst-mac
T2	☐	src-dst-mac
T3	☐	src-dst-mac
T4	☐	src-dst-mac
T5	☐	src-dst-mac
T6	☐	src-dst-mac
T7	☐	src-dst-mac
T8	☐	src-dst-mac
T9	☐	src-dst-mac
T10	☐	src-dst-mac
T11	☐	src-dst-mac
T12	☐	src-dst-mac

Port	Group
1	None
2	T1
3	T1
4	T1
5	T1
6	None
7	None
28	None

Apply Cancel

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

Port Authentication

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

18.1 Port Authentication Overview

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

- **IEEE 802.1x²** - An authentication server validates access to a port based on a username and password provided by the user.
- **MAC** - An authentication server validates access to a port based on the MAC address and password of the client.

Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See [Section 25.1.2 on page 244](#) for more information on configuring your RADIUS server settings.

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

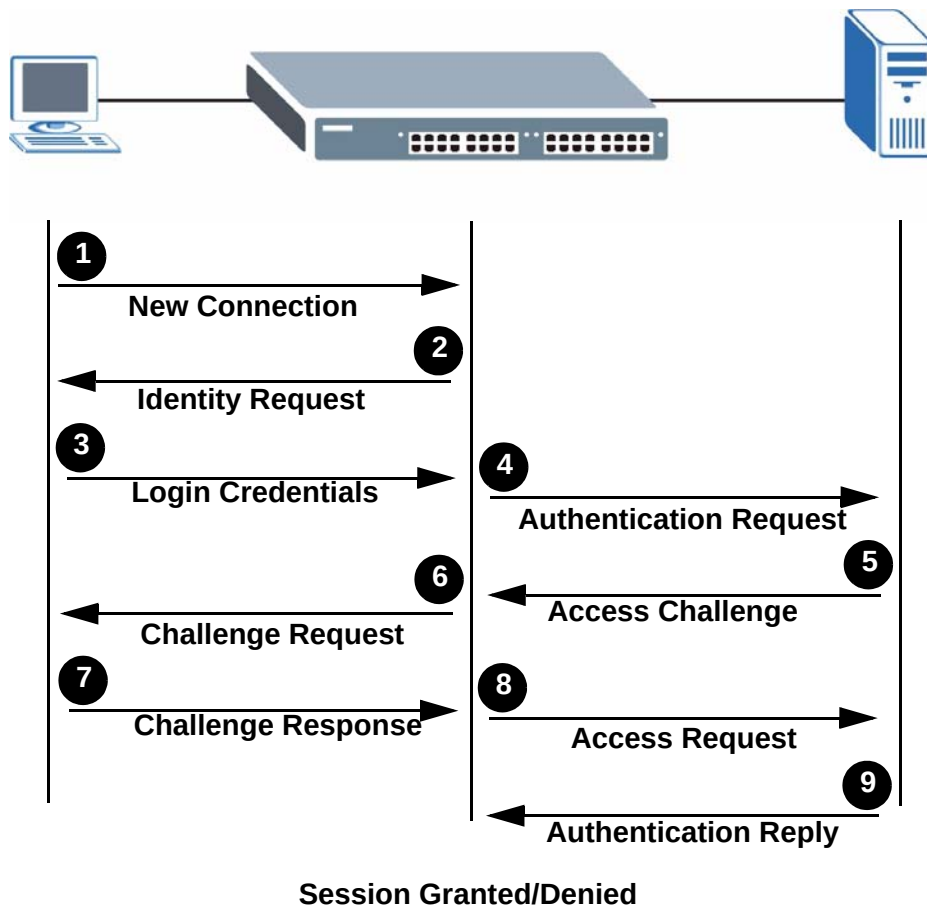
18.1.1 IEEE 802.1x Authentication

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

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.

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 78 IEEE 802.1x Authentication Process

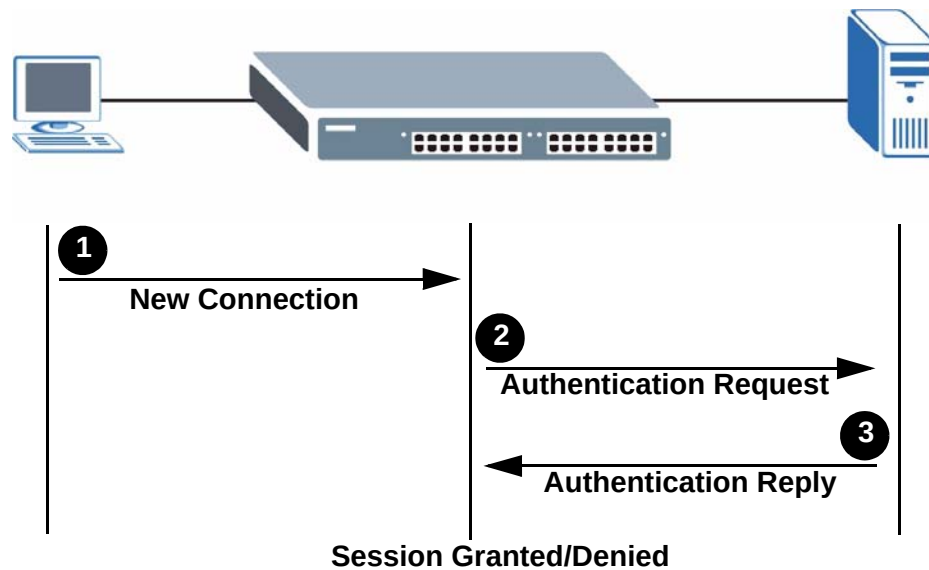


18.1.2 MAC Authentication

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

client connecting to a port on the Switch along with a password configured specifically for MAC authentication on the Switch.

Figure 79 MAC Authentication Process



18.2 Port Authentication Configuration

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

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

Figure 80 Advanced Application > Port Authentication



18.2.1 Activate IEEE 802.1x Security

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

Figure 81 Advanced Application > Port Authentication > 802.1x

Port	Active	Max-Req	Reauth	Reauth-period secs	Quiet-period secs	Tx-period secs	Supp-Timeout secs
*	☐		On				
1	☐	2	On	3600	60	30	30
2	☐	2	On	3600	60	30	30
3	☐	2	On	3600	60	30	30
4	☐	2	On	3600	60	30	30
5	☐	2	On	3600	60	30	30
6	☐	2	On	3600	60	30	30
7	☐	2	On	3600	60	30	30
8	☐	2	On	3600	60	30	30
9	☐	2	On	3600	60	30	30
27	☐	2	On	3600	60	30	30
28	☐	2	On	3600	60	30	30

Apply Cancel

The following table describes the labels in this screen.

Table 44 Advanced Application > Port Authentication > 802.1x

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

Table 44 Advanced Application > Port Authentication > 802.1x (continued)

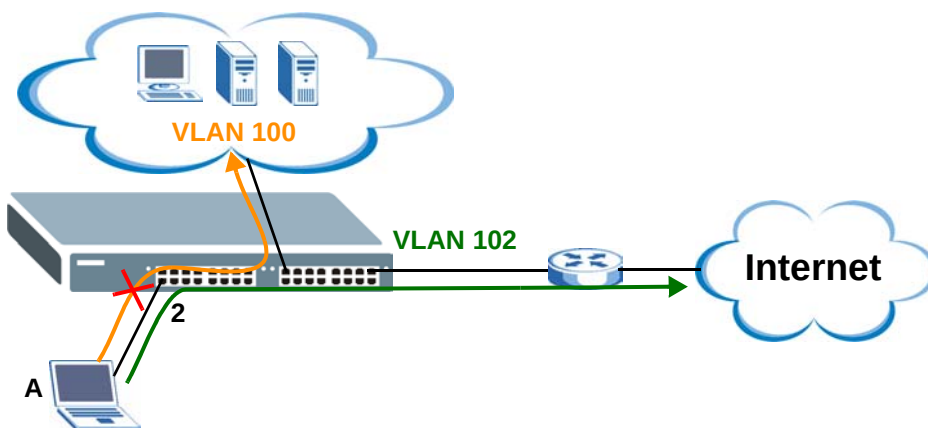
LABEL	DESCRIPTION
Max-Req	Specify the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.
Reauth	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-period	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Quiet-period	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

18.2.2 Guest VLAN

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

rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 82 Guest VLAN Example



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

Figure 83 Advanced Application > Port Authentication > 802.1x > Guest VLAN

Guest Vlan 802.1x

Port	Active	Guest Vlan	Host-mode	Multi-Secure Num
*	☐		Multi-Host	
1	☐	1	Multi-Host	1
2	☐	1	Multi-Host	1
3	☐	1	Multi-Host	1
4	☐	1	Multi-Host	1
5	☐	1	Multi-Host	1
6	☐	1	Multi-Host	1
7	☐	1	Multi-Host	1
8	☐	1	Multi-Host	1
9	☐	1	Multi-Host	1
10	☐	1	Multi-Host	1
27	☐	1	Multi-Host	1
28	☐	1	Multi-Host	1

The following table describes the labels in this screen.

Table 45 Advanced Application > Port Authentication > 802.1x > Guest VLAN

LABEL	DESCRIPTION
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 settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.
Guest Vlan	A guest VLAN is a pre-configured VLAN on the Switch that allows non-authenticated users to access limited network resources through the Switch. You must also enable IEEE 802.1x authentication on the Switch and the associated ports. Enter the number that identifies the guest VLAN. Make sure this is a VLAN recognized in your network.
Host-mode	Specify how the Switch authenticates users when more than one user connect to the port (using a hub). Select Multi-Host to authenticate only the first user that connects to this port. If the first user enters the correct credential, any other users are allowed to access the port without authentication. If the first user fails to enter the correct credential, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, rest of the users are blocked until a user does the authentication process again. Select Multi-Secure to authenticate each user that connects to this port.
Multi-Secure Num	If you set Host-mode to Multi-Secure , specify the maximum number of users (between 1 and 24) that the Switch will authenticate on this port.
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.

18.2.3 Activate MAC Authentication

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

Figure 84 Advanced Application > Port Authentication > MAC Authentication

Port	Active
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐

The following table describes the labels in this screen.

Table 46 Advanced Application > Port Authentication > MAC Authentication

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

Table 46 Advanced Application > Port Authentication > MAC Authentication

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, then this entry will not be deleted from the MAC address table. Note: If the Aging Time in the Switch Setup screen is set to a lower value, then it supersedes this setting. See Section 8.5 on page 108.
Port	This field displays a port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each 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 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 XGS-4728F can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K. The XGS-4526 or XGS-4528F can learn up to 8K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 8K.

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

19.2 Port Security Setup

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

Figure 85 Advanced Application > Port Security

Port Security VLAN MAC Address Limit

MAC Freeze :

Port List MAC freeze

Port Security :

Active ☐

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	☐	☒	0
1	☐	☒	0
2	☐	☒	0
3	☐	☒	0
4	☐	☒	0
5	☐	☒	0

Apply Cancel

The following table describes the labels in this screen.

Table 47 Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click MAC freeze , all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the Static MAC Forwarding screen.
MAC freeze	Click MAC freeze to have the Switch automatically select the Active check boxes and clear the Address Learning check boxes only for the ports specified in the Port list .
Active	Select this option to enable port security on the Switch.
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. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 47 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16384" in the XGS-4728F and from "0" to "8192" in the XGS-4526 or XGS-4528F. "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.

19.3 VLAN MAC Address Limit

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

Figure 86 Advanced Application > Port Security > VLAN MAC Address Limit

The screenshot shows the 'VLAN MAC Address Limit' configuration interface. At the top, there's a title bar with the text 'VLAN MAC Address Limit' and a link to 'Port Security'. Below this, there are four input fields: 'Active' with a checkbox, 'Port' with a text box, 'VID' with a text box, and 'Limit Number' with a text box. Underneath these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the screen, there is a table with the following columns: 'Index', 'Active', 'Port', 'VID', 'Limit Number', and 'Delete'. Below the table, there are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 48 Advanced Application > Port Security > VLAN MAC Address Limit

LABEL	DESCRIPTION
Active	Select this option to activate this rule.
Port	Enter the number of the port to which this rule is applied.
VID	Enter the VLAN identification number.
Limit Number	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port in a specified VLAN. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16384" in the XGS-4728F and from "0" to "8192" in the XGS-4526 or XGS-4528F. "0" means this feature is disabled.
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.
Active	This field displays Yes when the rule is activated and No when is it deactivated.
Port	This field displays the number of the port to which this rule is applied.
VID	This is the VLAN ID number to which the port belongs.
Limit Number	This is the maximum number of MAC addresses which a port can learn in a VLAN.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es) in the Delete column.

Classifier

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

20.1 About the Classifier and QoS

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

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

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

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed for a classified traffic flow (refer to [Chapter 21 on page 207](#) to configure policy rules).

20.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to [Chapter 21 on page 207](#).

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

Figure 87 Advanced Application > Classifier

Classifier

Active ☐

Name

Packet Format **All**

Layer 2

VLAN ☒ Any

Priority ☒ Any

Ethernet Type ☒ All (Hex)

Source MAC Address ☒ Any : : : : :

Port ☒ Any

Destination MAC Address ☒ Any : : : : :

Layer 3

DSCP ☒ Any

IP Protocol ☒ All Establish Only ☐

Source IP Address / Address Prefix /

Socket Number ☒ Any

Destination IP Address / Address Prefix /

Socket Number ☒ Any

Add Cancel Clear

Index	Active	Name	Rule	Delete

Delete Cancel

The following table describes the labels in this screen.

Table 49 Advanced Application > Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are All , 802.3 tagged , 802.3 untagged , Ethernet II tagged and Ethernet II untagged . A value of 802.3 indicates that the packets are formatted according to the IEEE 802.3 standards. A value of Ethernet II indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.

Table 49 Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
Layer 2	
Specify the fields below to configure a layer-2 classifier.	
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	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. Refer to Table 51 on page 205 for information.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (Any).
Destination	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3	
Specify the fields below to configure a layer-3 classifier.	
DSCP	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.
IP Protocol	Select an IP protocol type or select Other and enter the protocol number in decimal value. Refer to Table 52 on page 205 for more information. 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.
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.
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	
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.

Table 49 Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
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 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 begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.

20.3 Viewing and Editing Classifier Configuration

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

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

Figure 88 Advanced Application > Classifier: Summary Table

Index	Active	Name	Rule	Delete
<u>1</u>	Yes	Example	EtherType = IP; SrcMac = 00:50:ba:ad:4f:81; SrcPort = port 2;	☐

The following table describes the labels in this screen.

Table 50 Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
Rule	This field displays a summary of the classifier rule's settings.

Table 50 Classifier: Summary Table

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

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

Table 51 Common Ethernet Types and Protocol Number

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

Some of the most common IP ports are:

Table 52 Common IP Ports

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

20.4 Classifier Example

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

Figure 89 Classifier: Example

The screenshot shows the 'Classifier' configuration window. It is divided into two main sections: Layer 2 and Layer 3. The 'Active' checkbox is checked. The 'Name' field is set to 'Example'. The 'Packet Format' is set to 'All'. In the Layer 2 section, 'VLAN' is set to 'Any', 'Priority' is set to '0', and 'Ethernet Type' is set to 'All'. The 'Source' section is highlighted with a red circle, showing 'MAC Address' set to 'Any' and 'Port' set to '2'. The 'Destination' section shows 'MAC Address' set to 'Any'. In the Layer 3 section, 'DSCP' is set to 'Any', 'IP Protocol' is set to 'All' with 'Establish Only' unchecked, and 'Source' and 'Destination' sections are both set to 'Any' for 'IP Address / Address Prefix' and 'Socket Number'. At the bottom, there are 'Add', 'Cancel', and 'Clear' buttons. A red circle with the word 'EXAMPLE' is in the bottom right corner.

After you have configured a classifier, you can configure a policy to define action(s) on the classified traffic flow. See [Chapter 21 on page 207](#) for information on configuring a policy rule.

Policy Rule

This chapter shows you how to configure policy rules.

21.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 20 on page 201](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

21.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

21.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

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.

21.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to [Section 20.2 on page 201](#) for more information.

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

Figure 90 Advanced Application > Policy Rule

Policy

Active ☐

Name

Classifier(s)

Parameters

General

Egress Port

Priority

DSCP

TOS

Bandwidth Kbps

Metering

Out-of-Profile DSCP

Action

Forwarding

☒ No change

☐ Discard the packet

☐ Do not drop the matching frame previously marked for dropping

Priority

☒ No change

☐ Set the packet's 802.1p priority

☐ Send the packet to priority queue

☐ Replace the 802.1p priority field with the IP TOS value

Diffserv

☒ No change

☐ Set the packet's TOS field

☐ Replace the IP TOS field with the 802.1p priority value

☐ Set the Diffserv Codepoint field in the frame

Outgoing

☐ Send the packet to the mirror port

☐ Send the packet to the egress port

Metering

☐ Enable

Out-of-profile action

☐ Drop the packet

☐ Change the DSCP value

☐ Set Out-Drop Precedence

☐ Do not drop the matching frame previously marked for dropping

Add Cancel Clear

The following table describes the labels in this screen.

Table 53 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.

Table 53 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Classifier(s)	This field displays the active classifier(s) you configure in the Classifier screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters	
Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the Action field.	
General	
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 1 and 1000000.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action	
Specify the action(s) the Switch takes on the associated classified traffic flow.	
Forwarding	Select No change to forward the packets. Select Discard the packet to drop the packets. Select Do not drop the matching frame previously marked for dropping to retain the frames that were marked to be dropped before.
Priority	Select No change to keep the priority setting of the frames. Select Set the packet's 802.1p priority to replace the packet's 802.1p priority field with the value you set in the Priority field. Select Send the packet to priority queue to put the packets in the designated queue. Select Replace the 802.1p priority field with the IP TOS value to replace the packet's 802.1p priority field with the value you set in the TOS field.
Diffserv	Select No change to keep the TOS and/or DSCP fields in the packets. Select Set the packet's TOS field to set the TOS field with the value you configure in the TOS field. Select Replace the IP TOS with the 802.1p priority value to replace the TOS field with the value you configure in the Priority field. Select Set the Diffserv Codepoint field in the frame to set the DSCP field with the value you configure in the DSCP field.

Table 53 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
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.
Metering	Select Enable to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select Drop the packet to discard the out-of-profile traffic. Select Change the DSCP value to replace the DSCP field with the value specified in the Out of profile DSCP field. Select Set Out-Drop Precedence to mark out-of-profile traffic and drop it when network is congested. Select Do not drop the matching frame previously marked for dropping to queue the frames that are marked to be dropped.
Add	Click 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 begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.

21.3 Viewing and Editing Policy Configuration

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

Figure 91 Advanced Application > Policy Rule: Summary Table

Index	Active	Name	Classifier(s)	Delete
1	Yes	Test	Example;	☐

Delete
Cancel

The following table describes the labels in this screen.

Table 54 Policy: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays Yes when policy is activated and No when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

21.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to [Section 20.4 on page 206](#)).

Figure 92 Policy Example

Policy

Active ☒

Name

Classifier(s)

Parameters

General

Metering

Bandwidth Kbps

Out-of-Profile DSCP

Egress Port

Priority

DSCP

TOS

Action

Forwarding

☒ No change

☐ Discard the packet

☐ Do not drop the matching frame previously marked for dropping

Priority

☒ No change

☐ Set the packet's 802.1p priority

☐ Send the packet to priority queue

☐ Replace the 802.1p priority field with the IP TOS value

Diffserv

☒ No change

☐ Set the packet's TOS field

☐ Replace the IP TOS field with the 802.1p priority value

☐ Set the Diffserv Codepoint field in the frame

Outgoing

☐ Send the packet to the mirror port

☐ Send the packet to the egress port

Metering

☐ Enable

Out-of-profile action

☒ Drop the packet

☐ Change the DSCP value

☐ Set Out-Drop Precedence

☐ Do not drop the matching frame previously marked for dropping

Add Cancel Clear

EXAMPLE

Queuing Method

This chapter introduces the queuing methods supported.

22.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

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

22.1.1 Strictly Priority

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

22.1.2 Weighted Fair Queuing

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

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

$$2^{(\text{Weight} - 1)} \times 10 \text{ KB}$$

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

$$2^4 \times 10\text{KB} = 160 \text{ KB}$$

22.1.3 Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

22.2 Configuring Queuing

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

Figure 93 Advanced Application > Queuing Method

Port	Method	Weight								Hybrid-SPQ Lowest-Queue
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
*	SPQ									None
1	SPQ	1	2	3	4	5	6	7	8	None
2	SPQ	1	2	3	4	5	6	7	8	None
3	SPQ	1	2	3	4	5	6	7	8	None
4	SPQ	1	2	3	4	5	6	7	8	None
5	SPQ	1	2	3	4	5	6	7	8	None
6	SPQ	1	2	3	4	5	6	7	8	None
7	SPQ	1	2	3	4	5	6	7	8	None

Apply Cancel

The following table describes the labels in this screen.

Table 55 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.

Table 55 Advanced Application > Queuing Method (continued)

LABEL	DESCRIPTION
Method	Select SPQ (Strictly Priority Queuing), WFQ (Weighted Fair Queuing) or WRR (Weighted Round Robin). Strictly Priority services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth weight (the number you configure in the Weight field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.
Weight Q0-Q7	When you select WFQ or WRR enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Hybrid- SPQ Lowest- Queue	This field is applicable only when you select WFQ or WRR. Select a queue (Q0 to Q7) to have the Switch use SPQ to service the subsequent queue(s) after and including the specified queue for the 1000Base-T, 1000Base-X and 10 Gigabit Ethernet ports. For example, if you select Q5, the Switch services traffic on Q5, Q6 and Q7 using SPQ. Select None to always use WFQ or WRR.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

VLAN Stacking

This chapter shows you how to configure VLAN stacking on your Switch. See the chapter on VLANs for more background information on Virtual LAN

23.1 VLAN Stacking Overview

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

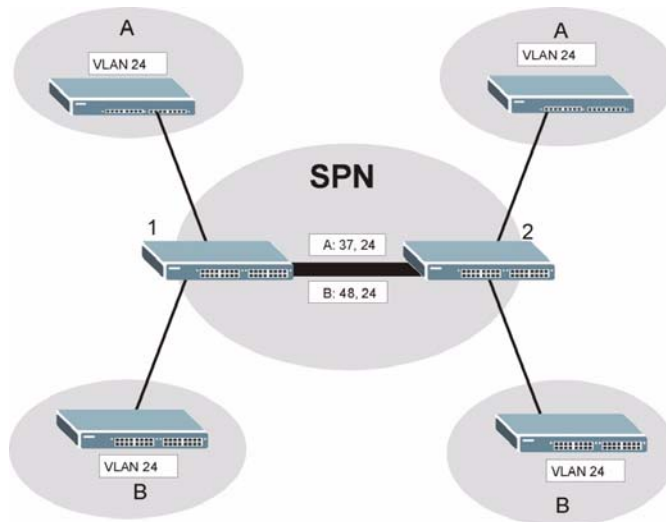
A service provider’s customers may require a range of VLANs to handle multiple applications. A service provider’s customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

23.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider’s Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to

distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 94 VLAN Stacking Example



23.2 VLAN Stacking Port Roles

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

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as “untagged”, so a second VLAN tag (outer VLAN tag) can be added.

Note: Static VLAN **Tx Tagging** MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by the Service Provider's (SP) VLAN ID (VID)).

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

23.3 VLAN Tag Format

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

Table 56 VLAN Tag Format

Type	Priority	VID

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

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

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

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the Switch, configure priority level of the inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

23.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the Switch **VLAN Stacking** screen.

Table 57 Single and Double Tagged 802.11Q Frame Format

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

Table 58 802.1Q Frame

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

23.4 Configuring VLAN Stacking

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

Figure 95 Advanced Application > VLAN Stacking

VLAN Stacking [Port-based QinQ](#) [Selective QinQ](#)

Active ☐

Port	Role	Tunnel TPID
*	Normal	
1	Normal	8100
2	Normal	8100
3	Normal	8100
4	Normal	8100
5	Normal	8100
6	Normal	8100

Apply Cancel

The following table describes the labels in this screen.

Table 59 Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the Switch.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Role	Select Normal to have the Switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in SPVID and Priority of the Port-based QinQ or the Selective QinQ screen are ignored. Select Access Port to have the Switch add the SP TPID tag to all incoming frames received on this port. Select Access Port for ingress ports at the edge of the service provider's network. Select Tunnel Port (available for Gigabit ports only) for egress ports at the edge of the service provider's network. Select Tunnel Port to have the Switch add the Tunnel TPID tag to all outgoing frames sent on this port. In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.
Tunnel TPID	TPID is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Enter a four-digit hexadecimal number from 0000 to FFFF that the Switch adds in the outer VLAN tag of the frames sent on the tunnel port(s). The Switch also uses this to check if the received frames are double-tagged. The value of this field is 0x8100 as defined in IEEE 802.1Q. If the Switch needs to communicate with other vendors' devices, they should use the same TPID. Note: You can define up to four different tunnel TPIDs (including 8100) in this screen at a time.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

23.4.1 Port-based Q-in-Q

Port-based Q-in-Q lets the Switch treat all frames received on the same port as the same VLAN flows and add the same outer VLAN tag to them, even they have different customer VLAN IDs.

Click **Port-based QinQ** in the **Advanced Application > VLAN Stacking** screen to display the screen as shown.

Figure 96 Advanced Application > VLAN Stacking > Port-based QinQ

Port	SPVID	Priority
*	1	0
1	1	0
2	1	0
3	1	0
4	1	0
5	1	0
6	1	0
7	1	0
8	1	0
9	1	0
10	1	0

Apply Cancel

The following table describes the labels in this screen.

Table 60 Advanced Application > VLAN Stacking > Port-based QinQ

LABEL	DESCRIPTION
Port	The port number identifies the port you are configuring.
SPVID	SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 9 on page 117 for more background information on VLAN ID.
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

23.4.2 Selective Q-in-Q

Selective Q-in-Q is VLAN-based. It allows the Switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags.

Note: Selective Q-in-Q rules are only applied to single-tagged frames received on the access ports. If the incoming frames are untagged or single-tagged but received on a tunnel port or cannot match any selective Q-in-Q rules, the Switch applies the port-based Q-in-Q rules to them.

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

Figure 97 Advanced Application > VLAN Stacking > Selective QinQ

The following table describes the labels in this screen.

Table 61 Advanced Application > VLAN Stacking > Selective QinQ

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	The port number identifies the port you are configuring.
CVID	Enter a customer VLAN ID (the inner VLAN tag) from 1 to 4094. This is the VLAN tag carried in the packets from the subscribers.
SPVID	SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 9 on page 117 for more background information on VLAN ID.
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the number of the selective VLAN stacking rule.
Active	This shows whether this rule is activated or not.
Name	This is the descriptive name for this rule.

Table 61 Advanced Application > VLAN Stacking > Selective QinQ (continued)

LABEL	DESCRIPTION
Port	This is the port number to which this rule is applied.
CVID	This is the customer VLAN ID in the incoming packets.
SPVID	This is the service provider's VLAN ID that adds to the packets from the subscribers.
Priority	This is the service provider's priority level in the packets.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

Multicast

This chapter shows you how to configure various multicast features.

24.1 Multicast Overview

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

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

24.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA website for more information).

24.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the Switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

24.1.3 IGMP Snooping

The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

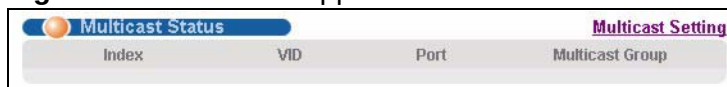
24.1.4 IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

24.2 Multicast Status

Click **Advanced Applications > Multicast** to display the screen as shown. This screen shows the multicast group information. See [Section 24.1 on page 227](#) for more information on multicasting.

Figure 98 Advanced Application > Multicast



Index	VID	Port	Multicast Group

The following table describes the labels in this screen.

Table 62 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.

24.3 Multicast Setting

Click **Advanced Applications > Multicast > Multicast Setting** link to display the screen as shown. See [Section 24.1 on page 227](#) for more information on multicasting.

Figure 99 Advanced Application > Multicast > Multicast Setting

Port	Immed. Leave	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	☐	☒ 4000	☐ 200	☐	0	Deny	Default	Auto
1	☐	☒ 4000	☐ 200	☐	0	Deny	Default	Auto
2	☐	☒ 4000	☐ 200	☐	0	Deny	Default	Auto
3	☐	☒ 4000	☐ 200	☐	0	Deny	Default	Auto
4	☐	☒ 4000	☐ 200	☐	0	Deny	Default	Auto
5	☐	☒ 4000	☐ 200	☐	0	Deny	Default	Auto
6	☐	☒ 4000	☐ 200	☐	0	Deny	Default	Auto

The following table describes the labels in this screen.

Table 63 Advanced Application > Multicast > Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP Snooping.
Active	Select Active to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Host Timeout	Specify the time (from 1 to 16 711 450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.

Table 63 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
IGMP Filtering	Select Active to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
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.
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 6,348,800) in milliseconds. 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, the Switch waits for IGMP reports after the multicast router 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 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.

Table 63 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6,348,800) in milliseconds. 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 sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select Deny to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select Replace to replace an existing entry in the multicast forwarding table with the new IGMP report(s) received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the Multicast > Multicast Setting > 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.

24.4 IGMP Snooping VLAN

Click **Advanced Applications > Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See [Section 24.1.4 on page 228](#) for more information on IGMP Snooping VLAN.

Figure 100 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

The screenshot shows the 'IGMP Snooping VLAN' configuration interface. At the top, there's a title bar with the text 'IGMP Snooping VLAN' and a link 'Multicast Setting'. Below the title bar, there's a 'Mode' section with two radio buttons: 'auto' (which is selected) and 'fixed'. Underneath the mode section are 'Apply' and 'Cancel' buttons. The next section is labeled 'VLAN' and contains two input fields: 'Name' and 'VID'. Below these fields are 'Add', 'Cancel', and 'Clear' buttons. At the bottom of the screen, there's a table with four columns: 'Index', 'Name', 'VID', and 'Delete'. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 64 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select auto to have the Switch learn multicast group membership information of any VLANs automatically. Select fixed to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either auto or fixed mode, the Switch can learn up to 16 VLANs (including up to five VLANs you configured in the MVR screen). For example, if you have configured one multicast VLAN in the MVR screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. Note: You must also enable IGMP snooping in the Multicast Setting 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.

Table 64 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN (continued)

LABEL	DESCRIPTION
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. Note: You cannot configure the same VLAN ID as in the MVR screen.
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 this to clear the fields.
Index	This is the number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

24.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Applications > Multicast > Multicast Setting > IGMP Filtering Profile** link to display the screen as shown.

Figure 101 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

Profile Name	Start Address	End Address
	224.0.0.0	224.0.0.0

Add Clear

Profile Name	Start Address	End Address	Delete Profile	Delete Rule
Default	0.0.0.0	0.0.0.0	☐	☐

Delete Cancel

The following table describes the labels in this screen.

Table 65 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast 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 Add to save the profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the 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.
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.

Table 65 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile (continued)

LABEL	DESCRIPTION
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the Delete Profile column, then click the Delete button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the Delete Rule column, then click the Delete button.
Cancel	Click Cancel to clear the Delete Profile/Delete Rule check boxes.

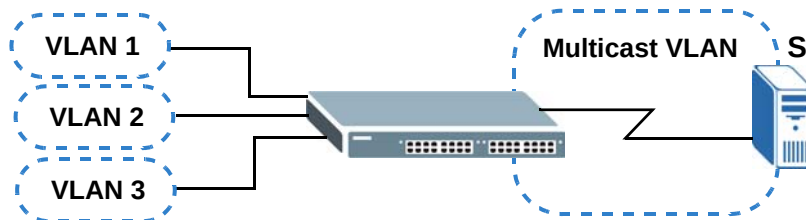
24.6 MVR Overview

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

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 102 MVR Network Example

24.6.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic.

Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

24.6.2 MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

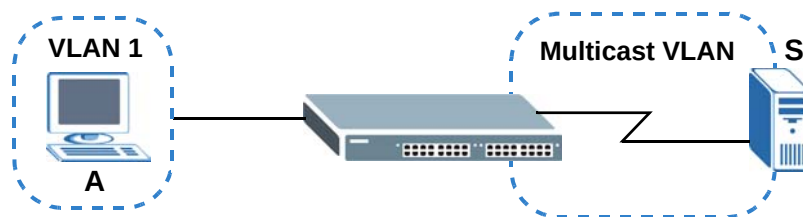
24.6.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, 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 103 MVR Multicast Television Example



24.7 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications > Multicast > Multicast Setting > MVR** link 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 104 Advanced Application > Multicast > Multicast Setting > MVR

The following table describes the related labels in this screen.

Table 66 Advanced Application > Multicast > Multicast Setting > 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.
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.

Table 66 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are Dynamic and Compatible . Select Dynamic to send IGMP reports to all MVR source ports in the multicast VLAN. Select Compatible to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click 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.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

24.8 MVR Group Configuration

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

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 105 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

The following table describes the labels in this screen.

Table 67 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

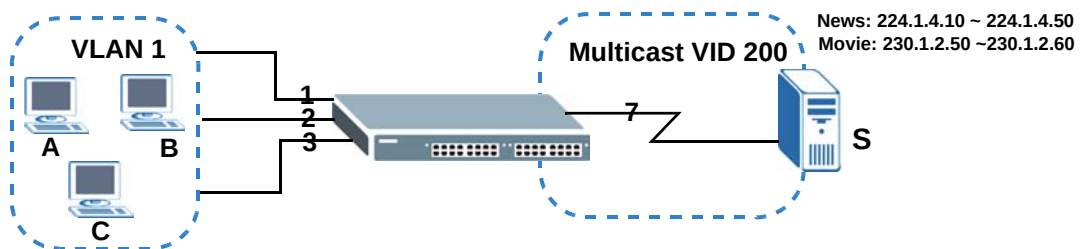
LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the MVR screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 24.1.1 on page 227 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the Start Address field if you want to configure only one IP address for a multicast group. Refer to Section 24.1.1 on page 227 for more information on IP multicast addresses.

Table 67 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

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.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select Delete All or Delete Group and click Delete to remove the selected entry(ies) from the table.
Cancel	Select Cancel to clear the checkbox(es) in the table.

24.8.1 MVR Configuration Example

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

Figure 106 MVR Configuration Example

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

Figure 107 MVR Configuration Example

MVR

Multicast SettingGroup Configuration

Active

☒

Name

Premium

Multicast VLAN ID

200

802.1p Priority

0

Mode

☒ Dynamic☐ Compatible

Port	Source Port	Receiver Port	None	Tagging
*		None		
1	☐	☒	☐	☐
2	☐	☒	☐	☐
3	☐	☒	☐	☐
4	☐	☐	☒	☐
5	☐	☐	☒	☐
6	☐	☐	☒	☐
7	☒	☐	☐	☒
8	☐	☐	☒	☐
9	☐	☐	☒	☐
10	☐	☐	☒	☐
11	☐	☐	☒	☐
12	☐	☐	☒	☐
13	☐	☐	☒	☐
14	☐	☐	☒	☐
15	☐	☐	☒	☐
16	☐	☐	☒	☐
17	☐	☐	☒	☐
18	☐	☐	☒	☐
19	☐	☐	☒	☐
20	☐	☐	☒	☐
21	☐	☐	☒	☐
22	☐	☐	☒	☐
23	☐	☐	☒	☐
24	☐	☐	☒	☐

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

Figure 108 MVR Group Configuration Example

Group Configuration MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
Movie	230.1.2.50	230.1.2.60

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	News	224.1.4.10	224.1.4.50	☐	☐

Delete Cancel

EXAMPLE

Figure 109 MVR Group Configuration Example

Group Configuration MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
	0.0.0.0	0.0.0.0

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	Movie	230.1.2.50	230.1.2.60	☐	☐
	News	224.1.4.10	224.1.4.50		☐

Delete Cancel

EXAMPLE

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

25.1 Authentication, Authorization and Accounting (AAA)

Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see [Section 25.1.2 on page 244](#)) and TACACS+ (Terminal Access Controller Access-Control System Plus, see [Section](#)

25.1.2 on page 244) as external authentication, authorization and accounting servers.

Figure 110 AAA Server



25.1.1 Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See [Chapter 46 on page 397](#)).

25.1.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 68 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, authorization, accounting or all of them on the Switch. First, configure your authentication and accounting server settings (RADIUS, TACACS+ or both) and then set up the authentication priority, activate authorization and configure accounting settings.

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

Figure 111 Advanced Application > AAA



25.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See [Section 25.1.2 on page 244](#) for more information on RADIUS servers and [Section 25.3 on page 254](#) for RADIUS attributes utilized by the authentication and accounting features on the Switch. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 112 Advanced Application > AAA > RADIUS Server Setup

The screenshot shows the RADIUS Server Setup page. At the top, there is a blue header with an orange circle icon and the text 'RADIUS Server Setup'. In the top right corner, there is a link labeled 'AAA'. The page is divided into two main sections: 'Authentication Server' and 'Accounting Server'.

Authentication Server

Mode: index-priority (dropdown menu)
 Timeout: 30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1812		☐
2	0.0.0.0	1812		☐

Apply Cancel

Accounting Server

Timeout: 30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1813		☐
2	0.0.0.0	1813		☐

Apply Cancel

The following table describes the labels in this screen.

Table 69 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field only applies if you configure multiple RADIUS servers. Select index-priority and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select round-robin to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using index-priority for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click Apply .
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.
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.

Table 69 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 accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

25.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See [Section 25.1.2 on page 244](#) for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 113 Advanced Application > AAA > TACACS+ Server Setup

TACACS+ Server Setup Auth and Acct

Authentication Server

Mode: index-priority

Timeout: 30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		☐
2	0.0.0.0	49		☐

Apply Cancel

Accounting Server

Timeout: 30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		☐
2	0.0.0.0	49		☐

Apply Cancel

The following table describes the labels in this screen.

Table 70 Advanced Application > AAA > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	This field is only valid if you configure multiple TACACS+ servers. Select index-priority and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server. Select round-robin to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server. If you are using index-priority for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is 49 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click Apply .
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.
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.

Table 70 Advanced Application > AAA > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ 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.

25.2.3 AAA Setup

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

Figure 114 Advanced Application > AAA > AAA Setup

AAA Setup AAA

Authentication

Type	Method 1	Method 2	Method 3
Privilege Enable	local	-	-
Login	local	-	-

Authorization

Type	Active	Method
Exec	☐	radius
Dot1x	☐	radius

Accounting

Update Period: minutes

Type	Active	Broadcast	Mode	Method	Privilege
System	☐	☐	-	radius	-
Exec	☐	☐	start-stop	radius	-
Dot1x	☐	☐	start-stop	radius	-
Commands	☐	☐	stop-only	tacacs+	0

Apply Cancel

The following table describes the labels in this screen.

Table 71 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.

Table 71 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Type	Set whether the Switch provides the following services to a user. • Exec: Allow an administrator which logs in the Switch through Telnet or SSH to have different access privilege level assigned via the external server. • Dot1x: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.
Method	Select whether you want to use RADIUS or TACACS+ for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the start-stop option for the Exec or Dot1x entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • System - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • Exec - Configure the Switch to send information when an administrator logs in and logs out via the console port, telnet or SSH. • Dot1x - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session. • Commands - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.
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.

Table 71 Advanced Application > AAA > AAA 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.

25.2.4 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (see the CLI Reference Guide for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID**: An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type**: A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data**: A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch. Note that these attributes only work when you enable authorization (see [Section 25.2.3 on page 249](#)).

Table 72 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = 890 Vendor-Type = 1 Vendor-data = ingress rate (Kbps in decimal format)

Table 72 Supported VSAs

FUNCTION	ATTRIBUTE
Egress Bandwidth Assignment	Vendor-Id = 890 Vendor-Type = 2 Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = 890 Vendor-Type = 3 Vendor-Data = "shell:priv-lvl=N" or Vendor-ID = 9 (CISCO) Vendor-Type = 1 (CISCO-AVPAIR) Vendor-Data = "shell:priv-lvl=N" where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

25.2.5 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that these attributes only work when you enable authorization (see [Section 25.2.3 on page 249](#)).

Table 73 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.

25.3 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication, and accounting elements in a user profile, which is stored on the RADIUS server. This section lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for RADIUS attributes used for accounting.

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

25.3.1 Attributes Used for Authentication

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

25.3.1.1 Attributes Used for Authenticating Privilege Access

User-Name

- the format of the User-Name attribute is **\$enab#\$**, where # is the privilege level (1-14)

User-Password

NAS-Identifier

NAS-IP-Address

25.3.1.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

25.3.1.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

25.3.2 Attributes Used for Accounting

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

25.3.2.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-Id

- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 2007041917210300000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

25.3.2.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

Table 74 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 75 RADIUS Attributes - Exec Events via Telnet/SSH

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

25.3.2.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

Table 76 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			✓

Table 76 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Acct-Input-Gigawords		✓	✓
Acct-Output-Gigawords		✓	✓

IP Source Guard

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

26.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

26.1.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

26.1.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

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

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

26.1.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 115 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-...-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

26.1.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See [Chapter 41 on page 361](#) for more information about DHCP relay option 82.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings ([Chapter 41 on page 361](#)).

26.1.1.4 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

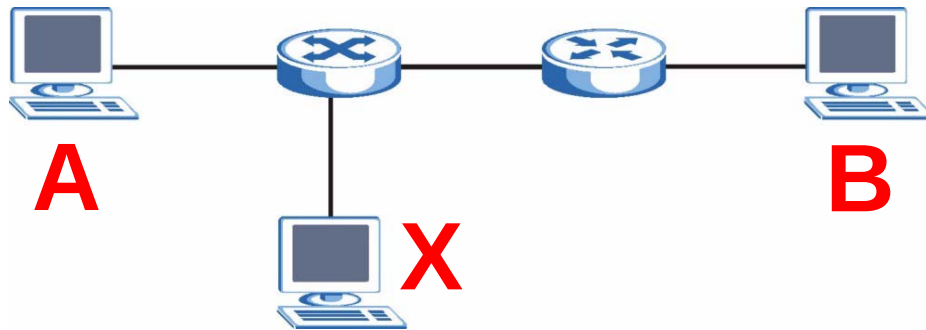
- 1 Enable DHCP snooping on the Switch.
- 2 Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.

- 3 Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
- 4 Configure static bindings.

26.1.2 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 116 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

26.1.2.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters ([Chapter 12 on page 145](#)).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.

- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

26.1.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

26.1.2.3 Syslog

The Switch can send syslog messages to the specified syslog server ([Chapter 48 on page 425](#)) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

26.1.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

- 1 Configure DHCP snooping. See [Section 26.1.1.4 on page 261](#).

Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

- 2 Enable ARP inspection on each VLAN.
- 3 Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

26.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns

the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 117 IP Source Guard

IP Source Guard						
Static Binding DHCP Snooping Arp Inspection						
Index	Mac Address	IP Address	Lease	Type	VID	Port
1	a1:12:12:12:12:01	172.23.37.222	infinity	static	1	18

The following table describes the labels in this screen.

Table 77 IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, 2d3h4m5s means the binding is still valid for 2 days, 3 hours, 4 minutes and 5 seconds. This field displays infinity if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. static: This binding was learned from information provided manually by an administrator. dhcp-snooping: This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

26.3 IP Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the

new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 118 IP Source Guard Static Binding

The following table describes the labels in this screen.

Table 78 IP Source Guard Static Binding

LABEL	DESCRIPTION
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select Any .
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. static : This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

Table 78 IP Source Guard Static Binding (continued)

LABEL	DESCRIPTION
Delete	Select this, and click Delete to remove the specified entry.
Cancel	Click this to clear the Delete check boxes above.

26.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

Figure 119 DHCP Snooping


DHCP Snooping

[Configure](#)

[IPSG](#)

Database Status

Description	Status	
Agent URL		
Write delay timer	300	seconds
Abort timer	300	seconds
Agent running	None	
Delay timer expiry	Not Running	
Abort timer expiry	Not Running	
Last succeeded time	None	
Last failed time	None	
Last failed reason	No failure recorded	
	Times	
Total attempts	0	
Startup failures	0	
Successful transfers	0	
Failed transfers	0	
Successful reads	0	
Failed reads	0	
Successful writes	0	
Failed writes	0	

Database detail

Description	Status
First successful access	None
Last ignored bindings counters	
Binding collisions	0
Invalid interfaces	0
Parse failures	0
Expired leases	0
Unsupported vlans	0
Last ignored time	None
Total ignored bindings counters	
Binding collisions	0
Invalid interfaces	0
Parse failures	0
Expired leases	0
Unsupported vlans	0

The following table describes the labels in this screen.

Table 79 DHCP Snooping

LABEL	DESCRIPTION
Database Status	
	This section displays the current settings for the DHCP snooping database. You can configure them in the DHCP Snooping Configure screen. See Section 26.5 on page 269 .
Agent URL	This field displays the location of the DHCP snooping database.
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.
Agent running	This field displays the status of the current update or access of the DHCP snooping database. none: The Switch is not accessing the DHCP snooping database. read: The Switch is loading dynamic bindings from the DHCP snooping database. write: The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays Not Running if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays Not Running if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.

Table 79 DHCP Snooping (continued)

LABEL	DESCRIPTION
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.
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.

Table 79 DHCP Snooping (continued)

LABEL	DESCRIPTION
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

26.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Figure 120 DHCP Snooping Configure

The screenshot shows the 'DHCP Snooping Configure' page. It features three tabs: 'Port', 'VLAN', and 'DHCP Snooping'. The 'DHCP Snooping' tab is active. Below the tabs, there is a section with 'Active' (checkbox) and 'DHCP Vlan' (dropdown menu). The 'Database' section contains 'Agent URL' (text input), 'Timeout interval' (300 seconds), and 'Write delay interval' (300 seconds). At the bottom, there is a 'Renew DHCP Snooping URL' (text input) with a 'Renew' button. 'Apply' and 'Cancel' buttons are located at the bottom center.

The following table describes the labels in this screen.

Table 80 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 enable Option82 in the DHCP Snooping VLAN Configure screen (Section 26.5.2 on page 272) 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 (Section 26.4 on page 266).
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.

26.5.1 DHCP Snooping Port Configure

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

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

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Figure 121 DHCP Snooping Port Configure

 DHCP Snooping Port Configure

Configure

Port	Server Trusted state	Rate (pps)
*	Untrusted	
1	Untrusted	0
2	Untrusted	0
3	Untrusted	0
4	Untrusted	0
5	Untrusted	0
6	Untrusted	0
7	Untrusted	0
8	Untrusted	0
	Untrusted	0

Apply

Cancel

The following table describes the labels in this screen.

Table 81 DHCP Snooping Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Server Trusted state	Select whether this port is a trusted port (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.

26.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information ([Chapter 41 on page 361](#)) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To

open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Figure 122 DHCP Snooping VLAN Configure

The following table describes the labels in this screen.

Table 82 DHCP Snooping VLAN Configure

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select 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.
Option82	Select this to have the Switch add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the DHCP Snooping Configure screen. See Section 26.5 on page 269 .
Information	Select this to have the Switch add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can configure the system name in the General Setup screen. See Chapter 8 on page 101 . You can specify the DHCP VLAN in the DHCP Snooping Configure screen. See Section 26.5 on page 269 .
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.

26.6 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 123 ARP Inspection Status

Index	MAC Address	VID	Port	Expiry (sec)	Reason	Delete
*	-	-	-	-	-	☐

Delete Cancel

The following table describes the labels in this screen.

Table 83 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).
Reason	This field displays the reason the ARP packet was discarded. MAC+VLAN: The MAC address and VLAN ID were not in the binding table. IP: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. Port: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this and click Delete to remove the specified entry.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the Delete check boxes above.

26.6.1 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Figure 124 ARP Inspection VLAN Status

The following table describes the labels in this screen.

Table 84 ARP Inspection VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (Start VID) and the highest VLAN ID (End VID) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

26.6.2 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 125 ARP Inspection Log Status



The following table describes the labels in this screen.

Table 85 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. See Section 26.7 on page 277 .

Table 85 ARP Inspection Log Status (continued)

LABEL	DESCRIPTION
Reason	This field displays the reason the log message was generated. dhcp deny: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. static deny: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. deny: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. dhcp permit: An ARP packet was forwarded because it matched a dynamic binding. static permit: An ARP packet was forwarded because it matched a static binding. In the ARP Inspection VLAN Configure screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 26.7.2 on page 280.
Time	This field displays when the log message was generated.

26.7 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 126 ARP Inspection Configure

ARP Inspection Configure

Port VLAN **ARP Inspection**

Active ☐

Filter Aging Time

Filter aging time 300 seconds

Log Profile

Log buffer size 32 entries

Syslog rate 5 entries

Log interval 1 seconds

Apply Cancel

The following table describes the labels in this screen.

Table 86 ARP Inspection Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Type 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified Syslog rate and Log interval. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click Clearing log status table in the ARP Inspection Log Status screen to clear the log and reset this counter. See Section 26.6.2 on page 276.
Syslog rate	Type the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the Log interval. You must configure the syslog server (Chapter 48 on page 425) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between Syslog rate and Log interval is illustrated in the following examples: 4 invalid ARP packets per second, Syslog rate is 5, Log interval is 1: the Switch sends 4 syslog messages every second. 6 invalid ARP packets per second, Syslog rate is 5, Log interval is 2: the Switch sends 5 syslog messages every 2 seconds.
Log interval	Type how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See Syslog rate for an example of the relationship between Syslog rate and Log interval .
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.

26.7.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 127 ARP Inspection Port Configure

Port	Trusted State	Rate (pps)	Limit Burst interval (seconds)
*	Untrusted		
1	Untrusted	15	1
2	Untrusted	15	1
3	Untrusted	15	1
4	Untrusted	15	1
5	Untrusted	15	1
6	Untrusted	15	1
7	Untrusted	15	1
8	Untrusted	15	1

Apply Cancel

The following table describes the labels in this screen.

Table 87 ARP Inspection Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port (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.

Table 87 ARP Inspection Port Configure (continued)

LABEL	DESCRIPTION
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.
Apply	Click 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.

26.7.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 128 ARP Inspection VLAN Configure

The following table describes the labels in this screen.

Table 88 ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.

Table 88 ARP Inspection VLAN Configure (continued)

LABEL	DESCRIPTION
Enabled	Select Yes to enable ARP inspection on the VLAN. Select No to disable ARP inspection on the VLAN.
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. None: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. Deny: The Switch generates log messages when it discards an ARP packet from the VLAN. Permit: The Switch generates log messages when it forwards an ARP packet from the VLAN. All: The Switch generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

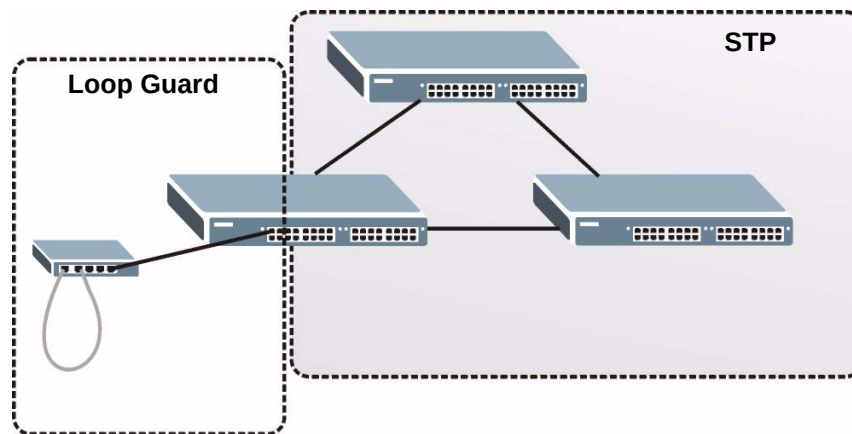
Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

27.1 Loop Guard Overview

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

Figure 129 Loop Guard vs STP



Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

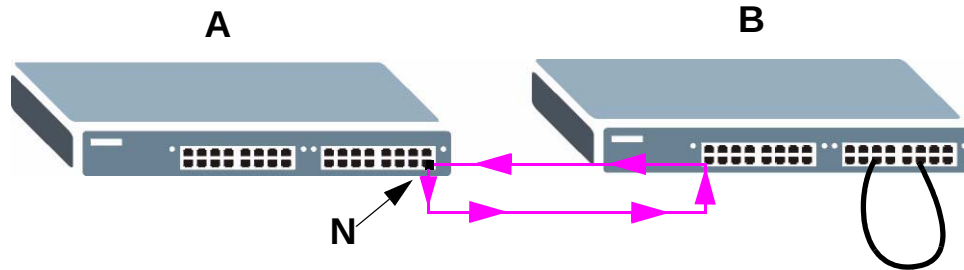
If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.

- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

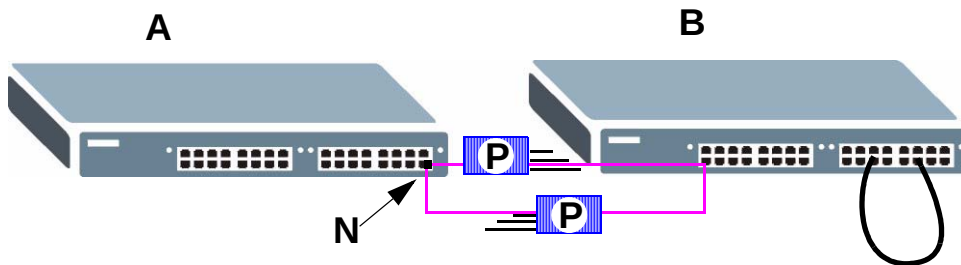
Figure 130 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

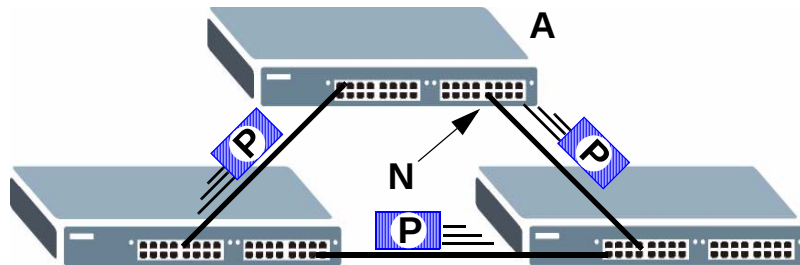
Figure 131 Loop Guard - Probe Packet



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 132 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 113](#)) or via commands (see the Ethernet Switch CLI Reference Guide).

27.2 Loop Guard Setup

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

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 133 Advanced Application > Loop Guard

Port	Active
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐

The following table describes the labels in this screen.

Table 89 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 a port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the Switch it is connected to is in loop state. If the Switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

VLAN Mapping

This chapter shows you how to configure VLAN mapping on the Switch.

28.1 VLAN Mapping Overview

With VLAN mapping enabled, the Switch can map the VLAN ID and priority level of packets received from a private network to those used in the service provider's network.

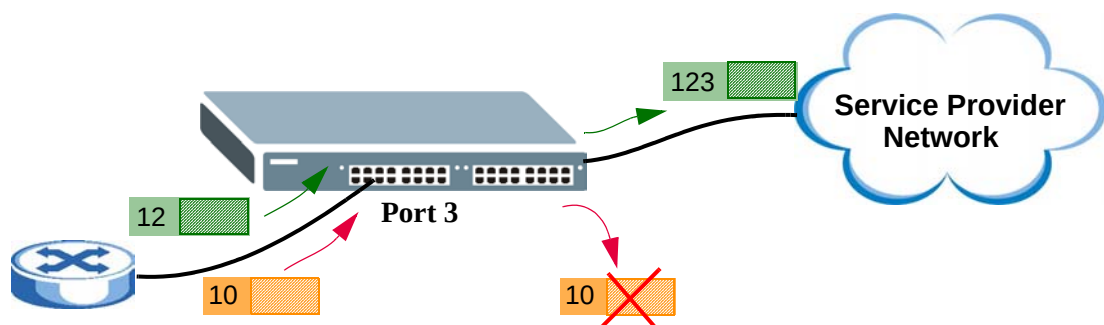
The Switch checks incoming traffic from the switch ports (non-management ports) against the VLAN mapping table first, the MAC learning table and then the VLAN table before forwarding them through the Gigabit uplink port. When VLAN mapping is enabled, the Switch discards the tagged packets that do not match an entry in the VLAN mapping table. If the incoming packets are untagged, the Switch adds a PVID based on the VLAN setting.

Note: You can not enable VLAN mapping and VLAN stacking at the same time.

28.1.1 VLAN Mapping Example

In the following example figure, packets that carry VLAN ID 12 and are received on port 3 match a pre-configured VLAN mapping rule. The Switch translates the VLAN ID from 12 into 123 before forwarding the packets. Any packets carrying a VLAN tag other than 12 (such as 10) and received on port 3 will be dropped.

Figure 134 VLAN mapping example



28.2 Enabling VLAN Mapping

Click **Advanced Application** and then **VLAN Mapping** in the navigation panel to display the screen as shown.

Figure 135 VLAN Mapping

Port	Active
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐
10	☐
12	☐

The following table describes the labels in this screen.

Table 90 VLAN Mapping

LABEL	DESCRIPTION
Active	Select this option to enable VLAN mapping on the Switch.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the VLAN mapping feature on this port. Clear this check box to disable the VLAN mapping feature.
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.

28.3 Configuring VLAN Mapping

Click the **VLAN Mapping Configure** link in the **VLAN Mapping** screen to display the screen as shown. Use this screen to enable and edit the VLAN mapping rule(s).

Figure 136 VLAN Mapping Configuration

The screenshot shows the 'VLAN Mapping Configure' interface. It includes a header with a logo and the title 'VLAN Mapping Configure', and a link 'VLAN Mapping'. The main form area contains several input fields: 'Active' with a checkbox, 'Name' with a text box, 'Port' with a text box, 'VID' with a text box, 'Translated VID' with a text box, and 'Priority' with a dropdown menu. Below these fields are 'Add' and 'Cancel' buttons. At the bottom of the screen is a table with columns: Index, Active, Name, Port, VID, Translated VID, Priority, and Delete. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 91 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 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.
Index	This is the number of the VLAN mapping entry in the table.
Active	This shows whether this entry is activated or not.
Name	This is the descriptive name for this rule.

Table 91 VLAN Mapping Configuration (continued)

LABEL	DESCRIPTION
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.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

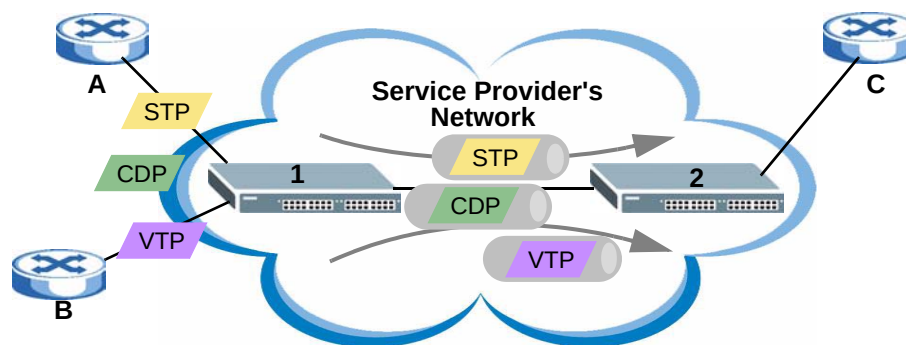
Layer 2 Protocol Tunneling

This chapter shows you how to configure layer-2 protocol tunneling on the Switch.

29.1 Layer 2 Protocol Tunneling Overview

Layer-2 protocol tunneling (L2PT) is used on the service provider's edge devices. L2PT allows edge switches (**1** and **2** in the following figure) to tunnel layer-2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) and VTP (VLAN Trunking Protocol) packets between customer switches (**A**, **B** and **C** in the following figure) connected through the service provider's network. The edge switch encapsulates layer-2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

Figure 137 Layer-2 Protocol Tunneling Network Scenario

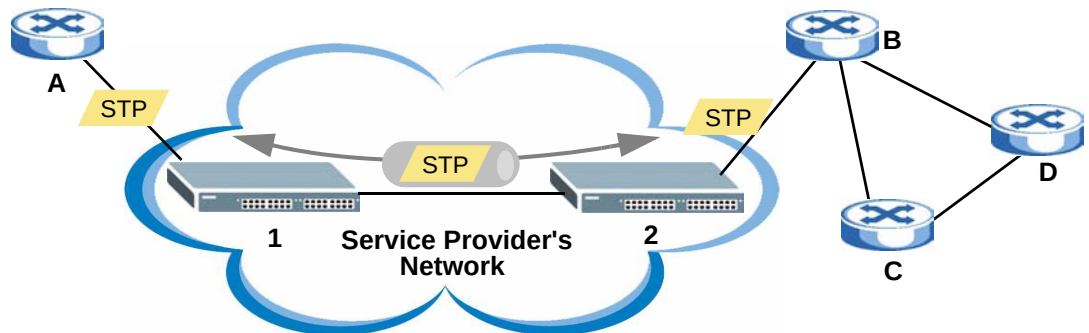


In the following example, if you enable L2PT for STP, you can have switches **A**, **B**, **C** and **D** in the same spanning tree, even though switch **A** is not directly connected to switches **B**, **C** and **D**. Topology change information can be propagated throughout the service provider's network.

To emulate a point-to-point topology between two customer switches at different sites, such as **A** and **B**, you can enable protocol tunneling on edge switches **1** and

2 for PAgP (Port Aggregation Protocol), LACP or UDLD (UniDirectional Link Detection).

Figure 138 L2PT Network Example



29.1.1 Layer-2 Protocol Tunneling Mode

Each port can have two layer-2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in [Figure 138 on page 292](#)) 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.

29.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application > Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 139 Advanced Application > Layer 2 Protocol Tunneling

Port	CDP	STP	VTP	Point to Point			Mode
				PAGP	LACP	UDLD	
*	☐	☐	☐	☐	☐	☐	Access
1	☐	☐	☐	☐	☐	☐	Access
2	☐	☐	☐	☐	☐	☐	Access
3	☐	☐	☐	☐	☐	☐	Access
4	☐	☐	☐	☐	☐	☐	Access
5	☐	☐	☐	☐	☐	☐	Access
6	☐	☐	☐	☐	☐	☐	Access
7	☐	☐	☐	☐	☐	☐	Access
8	☐	☐	☐	☐	☐	☐	Access
9	☐	☐	☐	☐	☐	☐	Access
10	☐	☐	☐	☐	☐	☐	Access
11	☐	☐	☐	☐	☐	☐	Access
12	☐	☐	☐	☐	☐	☐	Access
13	☐	☐	☐	☐	☐	☐	Access

The following table describes the labels in this screen.

Table 92 Advanced Application > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer-2 protocol tunneling on the Switch.
Destination MAC Address	Specify an MAC address with which the Switch uses to encapsulate the layer-2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number.

Table 92 Advanced Application > Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.
Point to Point	The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAgP and UDLD are Cisco's proprietary data link layer protocols. PAgP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.
PAGP	Select this option to have the Switch send PAgP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically creates and manages trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	Select Access to have the Switch encapsulate the incoming layer-2 protocol packets and forward them to the tunnel port(s). Select Access for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only. Select Tunnel for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer-2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the service(s) is not enabled on an access port, the protocol packets are dropped.
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.

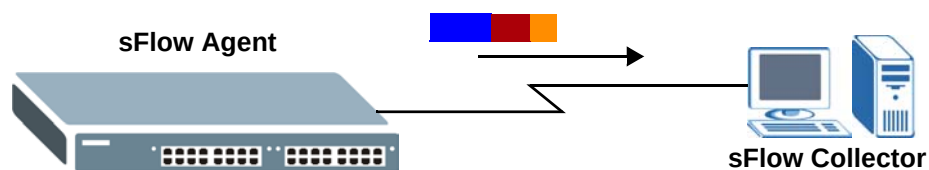
This chapter shows you how to configure sFlow to have the Switch monitor traffic in a network and send information to an sFlow collector for analysis.

30.1 sFlow Overview

sFlow (RFC 3176) is a standard technology for monitoring switched networks. An sFlow agent embedded on a switch or router gets sample data and packet statistics from traffic forwarded through its ports. The sFlow agent then creates sFlow data and sends it to an sFlow collector. The sFlow collector is a server that collects and analyzes sFlow datagram. An sFlow datagram includes packet header, input and output interface, sampling process parameters and forwarding information.

sFlow minimizes impact on CPU load of the Switch as it analyzes sample data only. sFlow can continuously monitor network traffic and create reports for network performance analysis and troubleshooting. For example, you can use it to know which IP address or which type of traffic caused network congestion.

Figure 140 sFlow Application



30.2 sFlow Port Configuration

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

Figure 141 Advanced Application > sFlow

Port	Active	Sample-rate	poll-interval	Collector Address
*	☐			
1	☐	32768	120	
2	☐	32768	120	
3	☐	32768	120	
4	☐	32768	120	
5	☐	32768	120	
6	☐	32768	120	
7	☐	32768	120	
27	☐	32768	120	
28	☐	32768	120	

The following table describes the labels in this screen.

Table 93 Advanced Application > sFlow

LABEL	DESCRIPTION
Active	Select this to enable the sFlow agent on the Switch.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to allow the Switch to monitor traffic on this port and generate and send sFlow datagram to the specified collector.

Table 93 Advanced Application > sFlow (continued)

LABEL	DESCRIPTION
Sample-rate	Enter a number (N) from 256 to 65535. The Switch captures every one out of N packets for this port and creates sFlow datagram.
poll-interval	Specify a time interval (from 20 to 120 in seconds) the Switch waits before sending the sFlow datagram and packet counters for this port to the collector.
Collector Address	Enter the IP address of the sFlow collector. Note: You must have the sFlow collector already configured in the sFlow > Collector screen. The sFlow collector does not need to be in the same subnet as the Switch, but it must be accessible from the Switch. Note: Configure UDP port 6343 (the default) on a NAT router to allow port forwarding if the collector is behind a NAT router. Configure a firewall rule for UDP port 6343 (the default) to allow incoming traffic if the collector is behind a firewall.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

30.2.1 sFlow Collector Configuration

Click the **Collector** link in the **sFlow** screen to display the screen as shown. You can configure up to four sFlow collectors in this screen. You may want to configure more than one collector if the traffic load to be monitored is more than one collector can manage.

Figure 142 Advanced Application > sFlow > Collector

The screenshot shows the 'sflow Collector' configuration interface. At the top, there's a header with the 'sflow' logo and a 'Collector' tab. Below the header, there are two input fields: 'Collector Address' with the value '0.0.0.0' and 'UDP Port' with the value '6343'. Under these fields are three buttons: 'Add', 'Cancel', and 'Clear'. Below these buttons is a horizontal line. At the bottom of the screen, there is a table with the following structure:

Index	Collector Address	UDP Port	Delete
1	1.2.3.4	6343	☐

Below the table, there are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

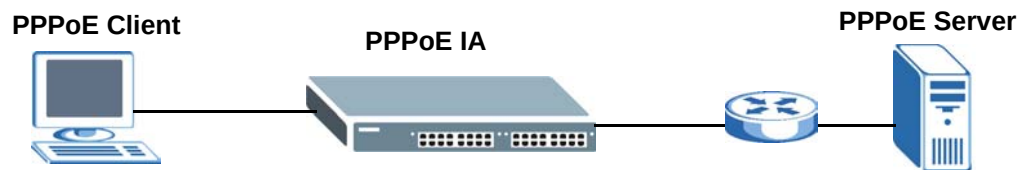
Table 94 Advanced Application > sFlow > Collector

LABEL	DESCRIPTION
Collector Address	Enter the IP address of the sFlow collector.
UDP Port	Enter a UDP port number the Switch uses to send sFlow datagram to the collector. If you change the port here, make sure you change it on the collector, too. The default port is 6343.
Add	Click 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 this entry.
Collector Address	This field displays IP address of the sFlow collector.
UDP Port	This field displays port number the Switch uses to send sFlow datagram to the collector.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to begin configuring this screen afresh.

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.

31.1 PPPoE Intermediate Agent Overview

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



31.1.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 95 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type	Tag_Len	Value	i1	i2
(0x0105)				

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.

31.1.2 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 96 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 97 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.

31.1.2.1 Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-option example is “Switch/07/0123” and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch's port 7 and belong to VLAN 123.

Table 98 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)

31.1.2.2 WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE > Intermediate Agent** screen, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates “Ethernet”.

Table 99 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)

31.1.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

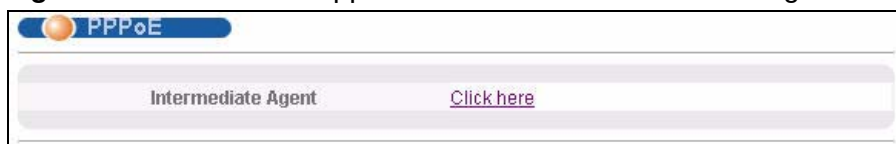
- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

31.2 The PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the Switch.

Click **Advanced Application** > **PPPoE** in the navigation panel to display the screen as shown. Click **Click Here** to go to the **Intermediate Agent** screen.

Figure 143 Advanced Application > PPPoE Intermediate Agent



31.3 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 144 Advanced Application > PPPoE > Intermediate Agent

The following table describes the labels in this screen.

Table 100 Advanced Application > PPPoE > Intermediate Agent

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the Switch.
access-node-identifier	Enter up to 20 ASCII characters to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.
circuit-id	Use this section to configure the Circuit ID field in the PADI and PADR packets. The Circuit ID you configure for a specific port or for a specific VLAN on a port has priority over this. The Circuit ID you configure for a specific port (in the Advanced Application > PPPoE > Intermediate Agent > Port screen) or for a specific VLAN on a port (in the Advanced Application > PPPoE > Intermediate Agent > Port > VLAN screen) has priority over this. That means, if you also want to configure PPPoE IA Per-Port or Per-Port Per-VLAN setting, leave the fields here empty and configure circuit-id and remote-id in the Per-Port or Per-Port Per-VLAN screen.
Active	Select this option to have the Switch add the user-defined identifier string and variables (specified in the option field) to PADI or PADR packets from PPPoE clients. If you leave this option unselected and do not configure any Circuit ID string (using CLI commands) on the Switch, the Switch will use the string specified in the access-node-identifier field.
identifier-string	Specify a string that the Switch adds in the Agent Circuit ID sub-option. You can enter up to 53 ASCII characters. Spaces are allowed.
option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include sp , sv , pv and spv which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value.
delimiter	Select a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. You can use a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

31.3.1 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 145 Advanced Application > PPPoE > Intermediate Agent > Port

Port	Server Trusted State	Circuit-id	Remote-id
*	Untrusted ▼		
1	Untrusted ▼		
2	Untrusted ▼		
3	Untrusted ▼		
4	Untrusted ▼		
5	Untrusted ▼		
6	Untrusted ▼		
7	Untrusted ▼		
8	Untrusted ▼		
9	Untrusted ▼		
10	Untrusted ▼		
11	Untrusted ▼		

Apply Cancel

The following table describes the labels in this screen.

Table 101 Advanced Application > PPPoE > Intermediate Agent > Port

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 101 Advanced Application > PPPoE > Intermediate Agent > Port (continued)

LABEL	DESCRIPTION
Server Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are uplink ports connected to PPPoE servers. • If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. • If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. • If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). • The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the Advanced Application > PPPoE > Intermediate Agent > Port > VLAN screen) has the highest priority.
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.

31.3.2 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 146 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

The following table describes the labels in this screen.

Table 102 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. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.

Table 102 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

LABEL	DESCRIPTION
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for 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.

31.3.3 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 147 Advanced Application > PPPoE > Intermediate Agent > VLAN

The screenshot displays the 'VLAN' configuration page under the 'Intermediate Agent' section. At the top, there's a 'Show VLAN' button and input fields for 'Start VID' and 'End VID'. Below these is an 'Apply' button. The main part of the screen is a table with the following columns: VID, Enabled, Circuit-id, and Remote-id. The table lists VLANs from 123 to 128, plus a '*' row for all. The 'Enabled' column contains dropdown menus with 'No' or 'Yes' selected. The 'Circuit-id' and 'Remote-id' columns contain checkboxes. In the row for VID 124, 'Yes' is selected in the 'Enabled' dropdown, and both the 'Circuit-id' and 'Remote-id' checkboxes are checked. At the bottom of the table, there are 'Apply' and 'Cancel' buttons.

VID	Enabled	Circuit-id	Remote-id
*	No	☐	☐
123	No	☐	☐
124	Yes	☒	☒
125	No	☐	☐
126	No	☐	☐
127	No	☐	☐
128	No	☐	☐

The following table describes the labels in this screen.

Table 103 Advanced Application > PPPoE > Intermediate Agent > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click Apply to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-id	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-id	Select this option to make the Remote ID settings for a specific VLAN take effect.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Error Disable

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.

32.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

32.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator or the commands. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

32.3 The Error Disable Screen

Use this screen to configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

Figure 148 Advanced Application > Errdisable

Errdisable	
CPU protection	Click here
Errdisable Detect	Click here
Errdisable Recovery	Click here

32.4 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 149 Advanced Application > Errdisable > CPU protection

CPU protection		Errdisable
Reason:	ARP	
Port	Rate Limit (pkt/s)	
*		
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
Apply Cancel		

The following table describes the labels in this screen.

Table 104 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. Note: Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. 0 means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. See Section 32.5 on page 311 for detailed information.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

32.5 Error-Disable Detect Configuration

Use 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 150 Advanced Application > Errdisable > Errdisable Detect

Cause	Active	Mode
*	☐	inactive-port
ARP	☐	inactive-port
BPDU	☐	inactive-port
IGMP	☐	inactive-port

Apply Cancel

The following table describes the labels in this screen.

Table 105 Advanced Application > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the Advanced Application > Errdisable > CPU protection screen. • inactive-port - The Switch disables the port on which the control packets are received. • inactive-reason - The Switch bypasses the processing of the specified control packets (such as ARP or IGMP packets), or drops all the specified control packets (such as BPDU) on the port. • rate-limitation - The Switch drops the additional control packets the port has to handle in every one second.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

32.6 Error-Disable Recovery Configuration

Use this screen to 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 151 Advanced Application > Errdisable > Errdisable Recovery

Reason	Timer Status	Interval
*	☐	
loopguard	☐	300
ARP	☐	300
BPDU	☐	300
IGMP	☐	300

Apply Cancel

The following table describes the labels in this screen.

Table 106 Advanced Application > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Select this option to turn on the error-disable recovery function on the Switch.
Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.
Timer Status	Select this option to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Private VLAN

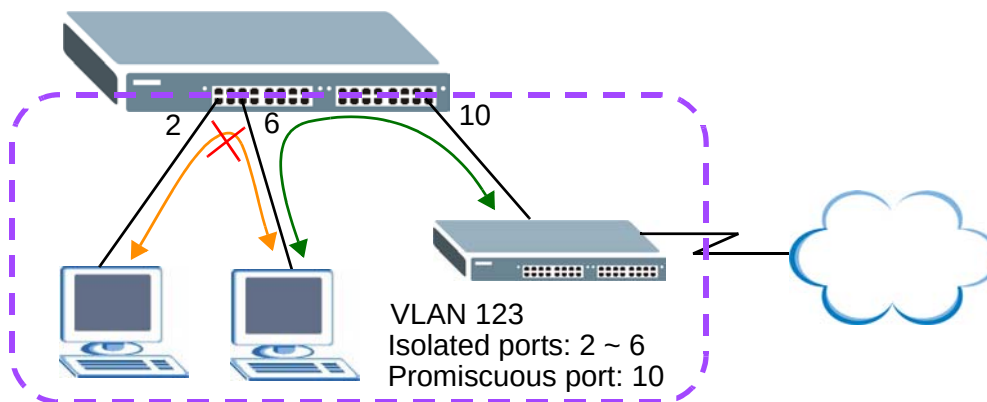
This chapter shows you how to configure the Switch to prevent communications between ports in a VLAN.

33.1 Private VLAN Overview

Private VLAN allows you to do port isolation within a VLAN in a simple way. You specify which port(s) 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 port(s) only.

Note: You can have up to one private VLAN rule for each VLAN.

Figure 152 Private VLAN Example



Note: Make sure you keep at least one port in the promiscuous port list for a VLAN with private VLAN enabled. Otherwise, this VLAN is blocked from the whole network.

33.2 Configuring Private VLAN

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

Figure 153 Advanced Application > Private VLAN

The following table describes the labels in this screen.

Table 107 Advanced Application > Private VLAN

LABEL	DESCRIPTION
Active	Check this box to enable private VLAN 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 port(s) 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 port(s) 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 port(s) that can communicate with any ports in the same VLAN.

Table 107 Advanced Application > Private VLAN (continued)

LABEL	DESCRIPTION
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

Static Route

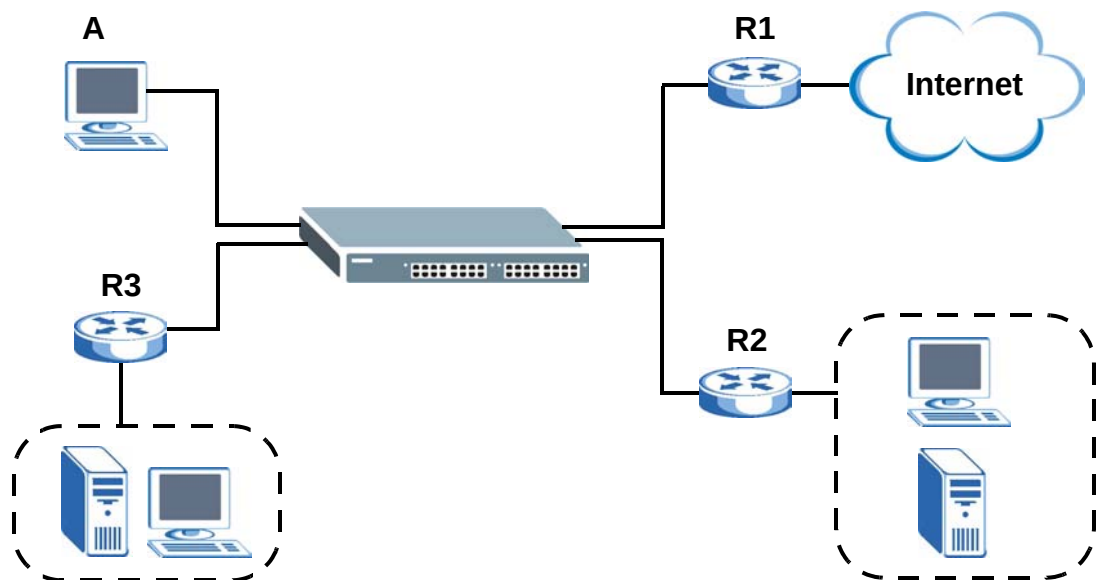
This chapter shows you how to configure static routes.

34.1 Static Routing Overview

The Switch usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Switch send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Switch. The Switch routes most traffic from **A** to the Internet through the Switch's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the Switch.

Figure 154 Example of Static Routing Topology



34.2 Configuring Static Routing

Click **IP Application > Static Routing** in the navigation panel to display the screen as shown.

Figure 155 IP Application > Static Routing

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	Example	172.21.1.1	255.255.0.0	192.168.1.2	2	☐

The following table describes the related labels you use to create a static route.

Table 108 IP Application > Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click Add to insert a new static route to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.

Table 108 IP Application > Static Routing (continued)

LABEL	DESCRIPTION
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays Yes when the static route is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is the immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

Policy Routing

This chapter shows you how to configure policy routing rules.

35.1 Policy Route Overview

Traditionally, routing is based on the destination address only and the Switch takes the shortest path to forward a packet. Policy routing provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets prior to the normal routing.

Individual routing policies are used as part of the overall policy routing process. A routing policy defines the action to take when a packet meets the criteria in a specified classifier. The action is taken only when all the criteria are met.

35.1.1 Benefits

- **Source-Based Routing** – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- **Cost Savings** – Policy routing allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- **Load Sharing** – Network administrators can use policy routing to distribute traffic among multiple paths.

35.2 Configuring Policy Routing Profile

Click **IP Application > Policy Routing** in the navigation panel to display the screen as shown. Use this screen to configure a policy routing profile, which can consist of multiple policy routing rules.

Figure 156 IP Application > Policy Routing

The screenshot shows the 'Policy Route' configuration interface. At the top, there's a header 'Policy Route' with a 'Rule Configuration' link. Below the header, there are two input fields: 'Active' with a checkbox and 'Profile Name' with a text box. Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. A table with four columns (Index, Active, Profile name, Delete) contains one row with Index '1', Active 'Yes', Profile name 'test', and a 'Delete' checkbox. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 109 IP Application > Policy Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this policy routing profile and rules in the profile.
Profile Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes. Spaces are allowed.
Add	Click Add to insert a new policy routing profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the policy routing profile. Click a number to edit the policy routing profile entry.
Active	This field displays Yes when the policy routing profile is activated and No when it is deactivated.
Profile Name	This field displays the descriptive name for this profile. This is for identification purposes only.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

35.2.1 Policy Routing Rule Configuration

You must first configure a layer-3 classifier in the **Classifier** screen (see [Section 20.2 on page 201](#)) and a policy routing profile in the **Policy Routing** screen (see [Section 35.2 on page 324](#)).

Use this screen to configure a policy route to override the default (shortest path) routing behavior and forward packets based on the classifier and action you specify. A policy route rule defines the matching classifier and the action to take when a packet meets the criteria in the classifier. The action is taken only when all the criteria are met. Policy-based routing is applied to incoming packets on a per interface basis before normal routing. The Switch does not perform normal routing on packets that match any of the policy routes.

Click **Rule Configuration** in the **IP Application > Policy Routing** screen to display the screen as shown.

Figure 157 IP Application > Policy Routing > Rule Configuration

Policy Route [Profile Configuration](#)

Profile Name: policyroute-1

Sequence:

Statement: ☒ Permit ☐ Deny

Classifier:

Action: Next Hop

Active	Profile name	Seq	State	Classifier	Rule Delete
Yes	policyroute-1	1	permit	class-2	☐

The following table describes the labels in this screen.

Table 110 IP Application > Policy Routing > Rule Configuration

LABEL	DESCRIPTION
Profile Name	This field displays the policy routing profile(s) you configure in the IP Application > Policy Routing screen. Select a profile for which you want to configure a policy routing rule.
Sequence	Enter the rule number from 1 to 64. The ordering of your rules is important as rules are applied in turn. You can not specify a number already in use by another rule.
Statement	Select Permit to forward traffic that matches this rule to the gateway specified in the rule. Select Deny to disable the rule action and forward traffic that matches this rule according to the routing table on the Switch.
Classifier	This field displays the available active classifiers you configure in the Classifier screen (see Chapter 20 on page 201), which are not used by any policy rule or policy routing rule. Select a classifier to which this policy routing rule applies.
Action	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Add	Click 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 begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.
Active	This field displays whether the policy route profile is enabled or not.
Profile Name	This field displays the name of the policy route profile with which the rule is associated.
Seq	This field displays the rule index number that you configure in the Sequence field. Click an index number to change the rule's Statement .
State	This field displays permit when the rule action is activated and deny when is it deactivated.
Classifier	This field displays the name of the classifier to which this policy applies.
Rule Delete	Select the policy routing rule(s) that you want to remove.
Delete	Click Delete to remove the selected entry(ies) from the summary table.
Cancel	Click Cancel to clear the Rule Delete check boxes.

This chapter shows you how to configure RIP (Routing Information Protocol).

36.1 RIP Overview

RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers. The **Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the Switch will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **Incoming** - the Switch will not send any RIP packets but will accept all RIP packets received.
- **Outgoing** - the Switch will send out RIP packets but will not accept any RIP packets received.
- **None** - the Switch will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Switch sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

36.1.1 Administrative Distance

When two or more than two different routing protocols, such as RIP and OSPF provide multiple routes to the same destination, the Switch can use the administrative distance of the route to determine which routing protocol to use and add the route to the routing table.

The lower the administrative distance value is, the more preferable the routing protocol is. If two routes have the same administrative distance value, the Switch

uses the route that has the lowest metric value. The following table lists the default administrative distance value of the route sources supported on the Switch.

Table 111 Default Distance Value

ROUTE SOURCE	ADMINISTRATIVE DISTANCE
Local	0
Static	1
OSPF	110
RIP	120

36.2 Configuring RIP

Click **IP Application > RIP** in the navigation panel to display the screen as shown. You cannot manually configure a new entry. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to [Section 8.6 on page 110](#)).

Figure 158 IP Application > RIP

The following table describes the labels in this screen.

Table 112 IP Application > RIP

LABEL	DESCRIPTION
Active	Select this check box to enable RIP on the Switch.
Distance	Enter a number from 10 to 255 to specify the administrative distance that is assigned to routes learned by RIP. The lower the administrative distance value is, the more preferable the routing protocol is. See Section 36.1.1 on page 327 for more information about administrative distance. Note: You cannot set two routing protocols to have the same administrative distance.
Index	This field displays the index number of an IP interface.

Table 112 IP Application > RIP (continued)

LABEL	DESCRIPTION
Network	This field displays the IP interface configured on the Switch. Refer to the section on IP Setup for more information on configuring IP domains.
Direction	Select the RIP direction from the drop-down list box. Choices are Outgoing , Incoming , Both and None .
Version	Select the RIP version from the drop-down list box. Choices are RIP-1 , RIP-2B and RIP-2M .
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 chapter describes the OSPF (Open Shortest Path First) routing protocol and shows you how to configure OSPF.

37.1 OSPF Overview

OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information.

OSPF offers some advantages over traditional vector-space routing protocols (such as RIP). The following table summarizes some of the major differences between OSPF and RIP.

Table 113 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metrics	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

37.1.1 OSPF Autonomous Systems and Areas

An OSPF autonomous system (AS) can be divided into logical areas. Each area represents a group of adjacent networks. All areas are connected to a backbone (also known as area 0). The backbone is the transit area to route packets between two areas. A stub area, at the edge of an AS is not a transit area since there is only one connection to the stub area.

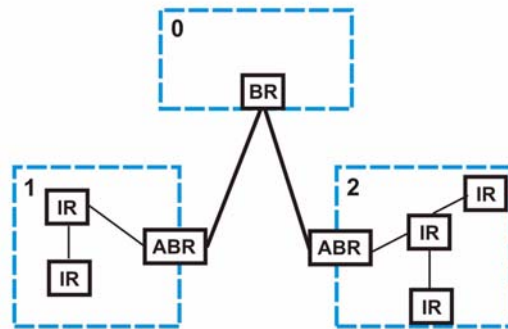
The following table describes the four classes of OSPF routers.

Table 114 OSPF: Router Types

TYPE	DESCRIPTION
Internal Router (IR)	An Internal or intra-area router is a router in an area.
Area Border Router (ABR)	An Area Border Router connects two or more areas.
Backbone Router (BR)	A backbone router has an interface to the backbone.
AS Boundary Router	An AS boundary router exchanges routing information with routers in other ASs.

The following figure depicts an OSPF network example. The backbone is area 0 with a backbone router. The internal routers are in area 1 and 2. The area border routers connect area 1 and 2 to the backbone.

Figure 159 OSPF Network Example



37.1.2 How OSPF Works

Layer-3 devices exchange routing information to build a synchronized link state database within the same AS or area. The link state database contains records of router IDs, their associated links and path costs. Each device can then use the link state database and Dijkstra algorithm to compute the least cost paths to network destinations.

Layer-3 devices build a synchronized link state database by exchanging Hello messages to confirm which neighbor (layer-3) devices exist and then they exchange database descriptions (DDs) to create the link state database. The link state database is constantly updated through LSAs (Link State Advertisements).

37.1.3 Interfaces and Virtual Links

An OSPF interface is a link between a layer-3 device and an OSPF network. An interface has state information, an IP address and subnet mask associated with it.

When you configure an OSPF interface, you first set an interface to transmit OSPF traffic and add the interface to an area.

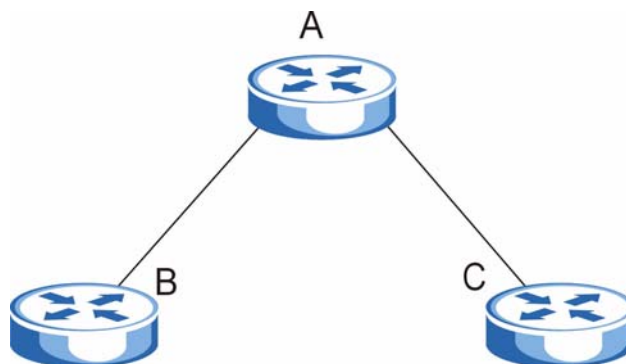
You can configure a virtual link to establish/maintain connectivity between a non-backbone area and the backbone. The virtual link must be configured on both layer-3 devices in the non-backbone area and the backbone.

37.1.4 OSPF and Router Elections

The OSPF protocol provides for automatic election of Designated Router (DR) and Backup Designated Router (BDR) on network segments. The DR and BDR keep track of link state updates in their area and make sure LSAs are sent to the rest of the network.

In most cases the default DR/BDR election is fine, but in some situations it must be controlled. In the following figure only router **A** has direct connectivity with all the other routers on the network segment. Routers **B** and **C** do not have a direct connection with each other. Therefore they should not be allowed to become DR or BDR. Only router **A** should become the DR.

Figure 160 OSPF Router Election Example



You can assign a priority to an interface which determines whether this router will be elected to be a DR or BDR. The router with the highest priority becomes the DR, while a router with a priority of 0 does not participate in router elections. In [Figure 160 on page 333](#) you can assign a priority of 0 to routers **B** and **C**, thereby ensuring they do not become DR or BDR and assign a priority of 1 to router **A** to make sure that it does become the DR.

37.1.5 Configuring OSPF

To configure OSPF on the Switch, do the following tasks:

- 1 Enable OSPF

- 2 Create OSPF areas
- 3 Create and associate interface(s) to an area
- 4 Create virtual links to maintain backbone connectivity.

37.2 OSPF Status

Use this screen to view current OSPF status. Click **IP Application > OSPF** in the navigation panel to display the screen as shown next. See [Section 37.1 on page 331](#) for more information on OSPF.

Figure 161 IP Application > OSPF Status

OSPF Status Configuration

OSPF: Running

Interface:

```

VLINK0 is down, line protocol is down
  OSPF is enabled, but not running on this interface
swif2 is up, line protocol is up
  Internet Address 192.168.1.10/24, Area 192.168.1.1
  Router ID 192.168.1.10, Network Type BROADCAST, Cost: 15
  Transmit Delay is 1 sec, State Backup, Priority 1
  
```

Neighbor:

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	Full/DR	00:00:34	192.168.1.1	swif2:192.168.

Link State Database:

```

OSPF Router with ID (192.168.1.10)
  Router Link States (Area 0.0.0.0)
  Link ID      ADV Router    Age  Seq#    CkSum  Link count
  
```

Poll Interval(s) Set Interval Stop

The following table describes the labels in this screen.

Table 115 IP Application > OSPF Status

LABEL	DESCRIPTION
OSPF	This field displays whether OSPF is activated (Running) or not (Down).
Interface	The text box displays the OSPF status of the interface(s) on the Switch.
Neighbor	The text box displays the status of the neighboring router participating in the OSPF network.

Table 115 IP Application > OSPF Status (continued)

LABEL	DESCRIPTION
Link State Database	The text box displays information in the link state database which contains data in the LSAs.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to end OSPF status polling.

The following table describes some common output fields.

Table 116 OSPF Status: Common Output Fields

FIELD	DESCRIPTION
Interface	
Internet Address	This field displays the IP address and subnet bits of an IP routing domain.
Area	This field displays the area ID.
Router ID	This field displays the unique ID of the Switch.
Transmit Delay	This field displays the transmission delay in seconds.
State	This field displays the state of the Switch (backup or DR (designated router)).
Priority	This field displays the priority of the Switch. This number is used in the designated router election.
Designated Router	This field displays the router ID of the designated router.
Backup Designated Router	This field displays the router ID of a backup designated router.
Time Intervals Configured	This field displays the time intervals (in seconds) configured.
Neighbor Count	This field displays the number of neighbor routers.
Adjacent Neighbor Count	This field displays the number of neighbor router(s) that is adjacent to the Switch.
Neighbor	
Neighbor ID	This field displays the router ID of the neighbor.
Pri	This field displays the priority of the neighbor. This number is used in the designated router election.
State	This field displays the state of the neighbor (backup or DR (designated router)).
Dead Time	This field displays the dead time in seconds.
Address	This field displays the IP address of a neighbor.
Interface	This field displays the MAC address of a device.
Link State Database	
Link ID	This field displays the ID of a router or subnet.
ADV Router	This field displays the IP address of the layer-3 device that sends the LSAs.

Table 116 OSPF Status: Common Output Fields (continued)

FIELD	DESCRIPTION
Age	This field displays the time (in seconds) since the last LSA was sent.
Seq #	This field displays the link sequence number of the LSA.
Checksum	This field displays the checksum value of the LSA.
Link Count	This field displays the number of links in the LSA.

37.3 OSPF Configuration

Use this screen to activate OSPF and set general settings. Click **IP Application > OSPF** and the **Configuration** link to display the **OSPF Configuration** screen. See [Section 37.1 on page 331](#) for more information on OSPF.

Figure 162 IP Application > OSPF Configuration: Activating and General Settings

The screenshot shows the 'OSPF Configuration' screen with the following settings:

- Active:** ☐ (unchecked)
- Router ID:** 0.0.0.0
- Distance:** 110
- Name:** name
- Area ID:** 0.0.0.0
- Authentication:** None
- Stub Network:** ☐ (unchecked)
- No Summary:** ☐ (unchecked)
- Default route cost:** 15

Buttons at the bottom include 'Apply', 'Cancel', 'Add', 'Cancel', 'Clear', 'Delete', and 'Cancel'.

The follow table describes the related labels in this screen.

Table 117 IP Application > OSPF Configuration: Activating and General Settings

LABEL	DESCRIPTION
Active	OSPF is disabled by default. Select this option to enable it.
Router ID	Router ID uniquely identifies the Switch in an OSPF. Enter a unique ID (that uses the format of an IP address in dotted decimal notation) for the Switch.

Table 117 IP Application > OSPF Configuration: Activating and General Settings

LABEL	DESCRIPTION
Distance	Enter a number from 10 to 255 to specify the administrative distance that is assigned to routes learned by OSPF. The lower the administrative distance value is, the more preferable the routing protocol is. See Section 36.1.1 on page 327 for more information about administrative distance. Note: You cannot set two routing protocols to have the same administrative distance.
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.

37.4 Configure OSPF Areas

To ensure that the Switch receives only routing information from a trusted layer-3 devices, activate authentication. The OSPF supports three levels of authentication:

- None – no authentication is used.
- Simple – authenticate link state updates using an 8 printable ASCII character password.
- MD5 – authenticate link state updates using a 16 printable ASCII character password.

To configure an area, set the related fields in the **OSPF Configuration** screen.

Figure 163 IP Application > OSPF Configuration: Area Setup

The following table describes the related labels in this screen.

Table 118 IP Application > OSPF Configuration: Area Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Enter a 32-bit ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. A value of 0.0.0.0 indicates that this is a backbone (also known as Area 0). You can create only one backbone area on the Switch.
Authentication	Select an authentication method (Simple or MD5) to activate authentication. Select None (default) to disable authentication. Usually interface(s) and virtual interface(s) should use the same authentication method as the associated area. If interface(s) and virtual interface(s) use different authentication methods than the associated area, the authentication methods are based on the interface(s) and virtual interface(s) settings.
Stub Network	Select this option to set the area as a stub area. If you enter 0.0.0.0 in the Area ID field, the settings in the Stub Area fields are ignored.
No Summary	Select this option to set the Switch to not send/receive LSAs.
Default Route Cost	Specify a cost (between 0 and 16777215) used to add a default route into a stub area for routes which are external to an OSPF domain. If you do not set a route cost, no default route is added.

Table 118 IP Application > OSPF Configuration: Area 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 set the above fields back to the factory defaults.

37.4.1 View OSPF Area Information Table

The bottom of the **OSPF Configuration** screen displays a summary table of all the OSPF areas you have configured.

Figure 164 IP Application > OSPF Configuration: Summary Table

Index	Name	Area ID	Authentication	Stub Network	Delete
1	Example	192.168.1.1	None	No	☐
Delete Cancel					

The following table describes the related labels in this screen.

Table 119 IP Application > OSPF Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of an area.
Name	This field displays the descriptive name of an area.
Area ID	This field displays the area ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. An area ID of 0.0.0.0 indicates the backbone.
Authentication	This field displays the authentication method used (None , Simple or MD5).
Stub Network	This field displays whether an area is a stub network (Yes) or not (No).
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

37.5 Configuring OSPF Redistribution

Use this screen to configure route redistribution and summary addresses. Route redistribution is used when other routers which use RIP routing protocol and/or static routes need to exchange routing information with the Switch using OSPF routing protocol. A summary address is used to cover more than one routing entries in order to reduce the routing table size.

In the **OSPF Configuration** screen, click **Redistribute** to display the **OSPF Redistribution** screen.

Figure 165 IP Application > OSPF Configuration > Redistribute

OSPF Redistribution [Configure](#)

Redistribute Route	Active	Type	Metric value
RIP	☐	1	15
Static	☐	1	15

[Apply](#) [Cancel](#)

Summary address

Subnet mask

[Add](#) [Cancel](#)

Index	Summary address	Subnet mask	Delete

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

Table 120 IP Application > OSPF Configuration > Redistribute

LABEL	DESCRIPTION
Redistribute Route	Route redistribution allows your Switch to import and translate external routes learned through RIP routing protocol or configured manually (Static) into the OSPF network transparently.
Active	Select this option to activate route redistribution for routes learned through the selected protocol.
Type	Select 1 for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the AB boundary router to the external metrics. Select 2 for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, the external cost of the AB boundary router is used in path decision to a destination.
Metric Value	Enter a route cost (between 0 and 16777215). The default metric value is 15.
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.

Table 120 IP Application > OSPF Configuration > Redistribute (continued)

LABEL	DESCRIPTION
Summary address	Enter a network IP address which can cover more than one network in order to reduce the routing table size. For example, you can use 192.168.8.0/22 instead of using 192.168.8.0/24, 192.168.9.0/24, 192.168.10.0/24, and 192.168.11.0/24. The third octet of these four network IP addresses is 00001000, 00001001, 00001010, 00001011 respectively. The first 6 digits (000010) are the common part among these IP addresses. So 192.168.8.0/22 can represent all of these networks.
Subnet mask	Enter the subnet mask for this summary IP address which can cover multiple networks.
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.

37.6 Configuring OSPF Interfaces

To configure an OSPF interface, first create an IP routing domain in the **IP Setup** screen (see [Section 8.6 on page 110](#) for more information). Once you create an IP routing domain, an OSPF interface entry is automatically created. See [Section 37.1 on page 331](#) for more information on OSPF.

In the **OSPF Configuration** screen, click **Interface** to display the **OSPF Interface** screen.

Figure 166 IP Application > OSPF Configuration > OSPF Interface

OSPF Interface Configuration

Network: 192.168.1.1/24
Area ID: 192.168.1.1
Authentication: None
Key ID: 1
Key:
Cost: 15
Priority: 1

Add Cancel Clear

Index	Network	Area ID	Authentication	Key ID	Cost	Priority	Delete
1	192.168.1.1/24	192.168.1.1	None	1	15	111	☐

Delete Cancel

The following table describes the labels in this screen.

Table 121 IP Application > OSPF Configuration > OSPF Interface

LABEL	DESCRIPTION
Network	Select an IP interface.
Area ID	Select the area ID (in an IP address format with dotted decimal notation) of an area to associate the interface to that area.
Authentication	Note: OSPF Interface(s) must use the same authentication method within the same area. Select an authentication method. The choices are Same-as-Area, None (default), Simple and MD5. To participate in an OSPF network, you must make the authentication method and/or password settings the same as the associated area. Select Same-as-Area to use the same authentication method within the area and set the related fields when necessary. Select None to disable authentication. This is the default setting. Select Simple and set the Key field to authenticate OSPF packets transmitted through this interface using simple password authentication. Select MD5 and set the Key ID and Key fields to authenticate OSPF packets transmitted through this interface using MD5 authentication.
Key ID	When you select MD5 in the Authentication field, specify the identification number of the authentication you want to use.
Key	When you select Simple in the Authentication field, enter a password eight-character long. Characters after the eighth character will be ignored. When you select MD5 in the Authentication field, enter a password 16-character long.
Cost	The interface cost is used for calculating the routing table. Enter a number between 0 and 65535. The default interface cost is 15.
Priority	The priority you assign to the interface is used in router elections to decide which router is going to be the Designated Router (DR) or the Backup Designated Router (BDR). You can assign a number between 0 and 255. A priority of 0 means that the router will not participate in router elections.
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 set the above fields back to the factory defaults.
Index	This field displays the index number for an interface.
Network	This field displays the IP interface information.
Area ID	This field displays the area ID (in an IP address format with dotted decimal notation) of an area to associate the interface to that area.
Authentication	This field displays the authentication method used (Same-as-Area , None , Simple or MD5).

Table 121 IP Application > OSPF Configuration > OSPF Interface (continued)

LABEL	DESCRIPTION
Key ID	When the Authentication field displays MD5 , this field displays the identification number of the key used.
Cost	This field displays the interface cost used for calculating the routing table.
Priority	This field displays the priority for this OSPF interface.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to begin configuring this screen afresh.

37.7 OSPF Virtual-Links

Configure and view virtual link settings in this screen. See [Section 37.1 on page 331](#) for more information on OSPF.

In the **OSPF Configuration** screen, click **Virtual-Link** to display the screen as shown next.

Figure 167 IP Application > OSPF Configuration > OSPF Virtual Link

The following table describes the related labels in this screen.

Table 122 IP Application > OSPF Configuration > OSPF Virtual Link

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Select the area ID (in an IP address format with dotted decimal notation) of an area to associate the interface to that area.
Peer Router ID	Enter the ID of a peer border router.

Table 122 IP Application > OSPF Configuration > OSPF Virtual Link (continued)

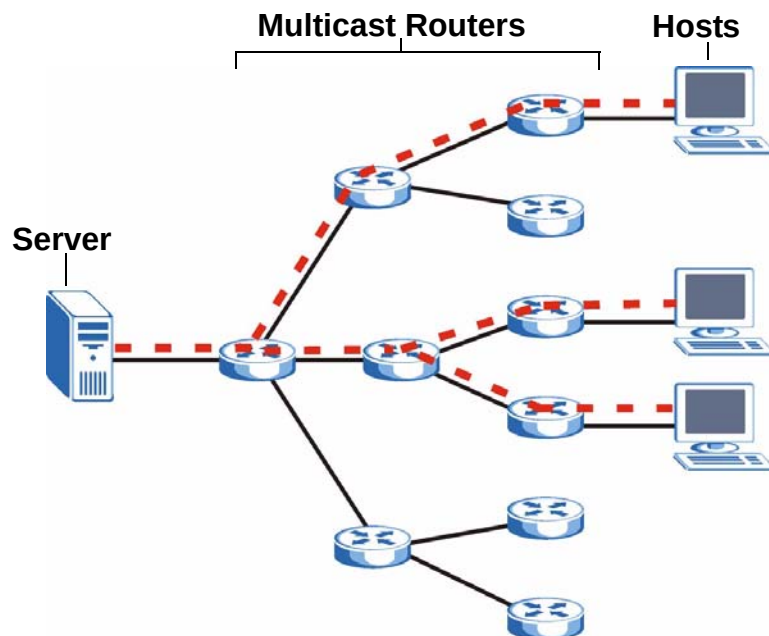
LABEL	DESCRIPTION
Authentication	Note: Virtual interface(s) must use the same authentication method within the same area. Select an authentication method. The choices are Same-as-Area, None (default), Simple and MD5. To exchange OSPF packets with a peer border router, you must make the authentication method and/or password settings the same as the peer border router. Select Same-as-Area to use the same authentication method within the area and set the related fields when necessary. Select None to disable authentication. This is the default setting. Select Simple to authenticate OSPF packets transmitted through this interface using a simple password. Select MD5 to authenticate OSPF packets transmitted through this interface using MD5 authentication.
Key ID	When you select MD5 in the Authentication field, specify the identification number of the authentication you want to use.
Key	When you select Simple in the Authentication field, enter a password eight-character long. When you select MD5 in the Authentication field, enter a password 16-character long.
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 set the above fields back to the factory defaults.
Index	This field displays an index number of an entry.
Name	This field displays a descriptive name of a virtual link.
Peer Router ID	This field displays the ID (that uses the format of an IP address in dotted decimal notation) of a peer border router.
Authentication	This field displays the authentication method used (Same-as-Area , None , Simple or MD5).
Key ID	When the Authentication field displays MD5 , this field displays the identification number of the key used.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

This chapter shows you how to configure the Switch as a multicast router. See also [Section 24.4 on page 232](#) for information on IGMP snooping.

38.1 IGMP Overview

IP multicast is an IETF standard for distributing data to multiple recipients. The following figure shows a multicast session and the relationship between a multicast server, multicast routers and multicast hosts. A multicast server transmits multicast packets and multicast routers forward multicast packets to multicast hosts.

Figure 168 IP Multicast



A host can decide to join or leave a multicast group at any time. A host can also be a member of more than one multicast group. Multicast groups are identified by IP addresses in the Class D range (224.0.0.0 to 239.255.255.255). A multicast server sends packets addressed to a particular multicast group (multicast IP address).

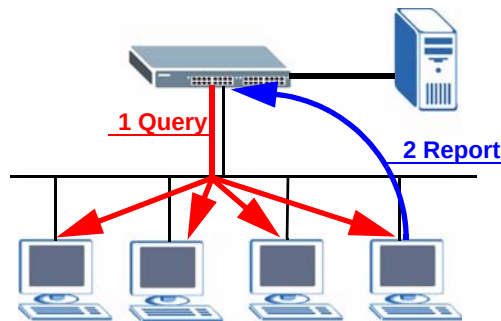
IGMP (Internet Group Management Protocol) is used by multicast hosts to indicate their multicast group membership to multicast routers. Multicast routers can also use IGMP to periodically check if multicast hosts still want to receive transmission from a multicast server. In other words, multicast routers check if any hosts on their network are still members of a specific multicast group.

The Switch supports IGMP version 1 (**IGMP-v1**), version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively. At start up, the Switch queries all directly connected networks to gather group membership. After that, the Switch periodically updates this information.

38.1.1 How IGMP Works

This section describes how IGMP works and the changes it has gone through from version 1 to version 3. IGMP version 1 defines how a multicast router checks to see if any multicast hosts are part of a multicast group. It checks for group membership by sending out an IGMP Query packet. Hosts that are members of a multicast group reply with an IGMP Report packet. This is also referred to as a join group request. The multicast router then keeps a list of all networks that have members of this multicast group and forwards multicast traffic to that network.

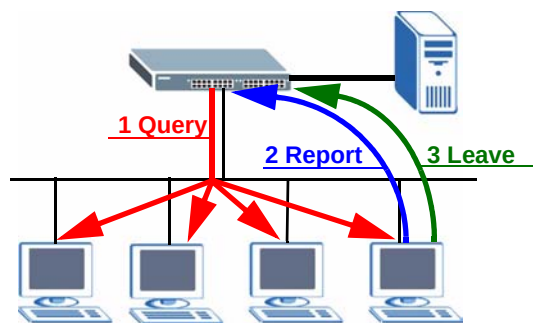
Figure 169 IGMP Version 1 Example



The main difference in IGMP version 2 is that it provides a mechanism for a multicast group member to notify a multicast router that it is leaving a multicast group. The multicast router then sends a group-specific IGMP query to check if there are any members remaining in that group. If the multicast router does not receive an IGMP report from any members, it stops sending multicast traffic to that group. This change helps shorten the leave convergence time, in other words, the amount of time that a multicast router believes that there are group members

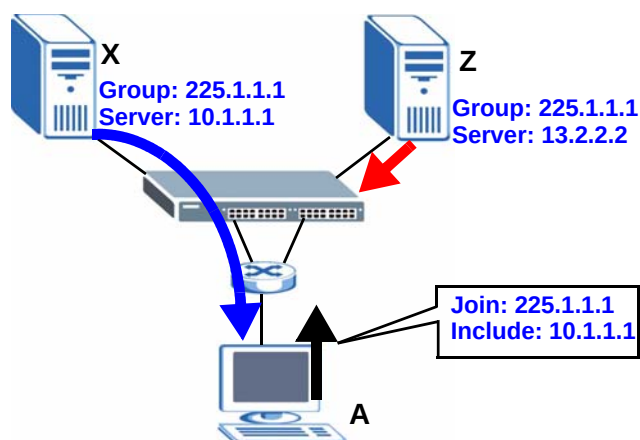
on a particular network. This in turn helps reduce the amount of multicast traffic going through the multicast router.

Figure 170 IGMP Version 2 Example



IGMP version 3 allows a multicast host to join a multicast group and specify from which source (multicast server) it wants to receive multicast packets. Alternatively, a multicast host can specify from which multicast servers it does not want to receive multicast packets. In the following figure multicast server **X** (IP address **10.1.1.1**) and multicast server **Z** (IP address **13.2.2.2**) both send multicast traffic to the same multicast group identified by the multicast IP address **225.1.1.1**. In IGMP version 3 multicast host **A** can join multicast group **225.1.1.1** and specify that it only wants to receive multicast packets from server **X**.

Figure 171 IGMP Version 3 Example



38.2 Port-based IGMP

The Switch sends IGMP Query packets to all ports. The Switch then listens for IGMP Report packets, and it records which port the messages came from. It then delivers multicast traffic to only those ports from which it received a request to join a multicast group.

38.3 Configuring IGMP

Click **IP Application > IGMP** in the navigation panel to display the screen as shown next. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to [Section 8.6 on page 110](#)).

Figure 172 IP Application > IGMP

Index	Network	Version
1	172.23.37.209/24	None
2	192.168.1.1/24	None

The following table describes the labels in this screen.

Table 123 IP Application > IGMP

LABEL	DESCRIPTION
Active	Select this check box to enable IGMP on the Switch. Note: You cannot enable both IGMP snooping and IGMP at the same time. Refer to Section 24.4 on page 232 for more information on IGMP snooping.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Unknown multicast frames are addressed to multicast groups for which the Switch has not recorded any group members. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Index	This field displays an index number of an entry.
Network	This field displays the IP domain configured on the Switch. Refer to Section 8.6 on page 110 for more information on configuring IP domains.
Version	Select an IGMP version from the drop-down list box. The choices are IGMP-v1 , IGMP-v2 , IGMP-v3 and None . Generally, if you want to enable IGMP on the Switch, you should choose IGMP-v3 as it is compatible with older versions. Choose an earlier version of IGMP (IGMP-v2 or IGMP-v1) if the multicast hosts on your network can not recognize IGMP version 3 or version 2 Query 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.

DVMRP

This chapter introduces DVMRP and tells you how to configure it.

39.1 DVMRP Overview

DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). This DVMRP implementation is based on draft-ietf-idmr-dvmrp-v3-10. DVMRP provides multicast forwarding capability to a layer-3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol. The DVMRP metric is a hop count of 32.

IGMP is a protocol used for joining or leaving a multicast group. You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in [Figure 175 on page 351](#).

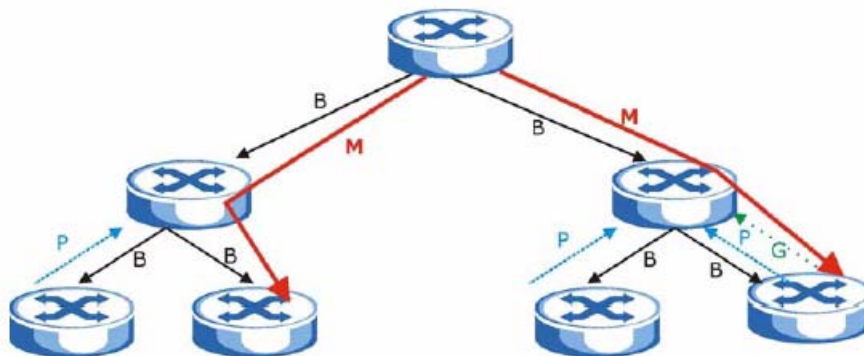
39.2 How DVMRP Works

DVMRP uses the Reverse Path Multicasting (RPM) algorithm to generate an IP Multicast delivery tree. Multicast packets are forwarded along these multicast tree branches. DVMRP dynamically learns host membership information using Internet Group Management Protocol (IGMP). The trees are updated dynamically to track the membership of individual groups.

- 1 Initially an advertisement multicast packet is broadcast ("**B**" in the following figure).
- 2 DVMRP-enabled Layer-3 devices that do not have any hosts in their networks that belong to this multicast group send back a prune message ("**P**").
- 3 If hosts later join the multicast group, a graft message ("**G**") to undo the prune is sent to the parent.

- 4 The final multicast (“M”) after pruning and grafting is shown in the next figure.

Figure 173 How DVMRP Works



39.2.1 DVMRP Terminology

DVMRP probes are used to discover other DVMRP Neighbors on a network.

DVMRP reports are used to exchange DVMRP source routing information. These packets are used to build the DVMRP multicast routing table that is used to build source trees and also perform Reverse Path Forwarding (RPF) checks on incoming multicast packets. RPF checks prevent duplicate packets being filtered when loops exist in the network topology.

DVMRP prunes trim the multicast delivery tree(s). DVMRP grafts attach a branch back onto the multicast delivery tree.

39.3 Configuring DVMRP

Configure DVMRP on the Switch when you wish it to act as a multicast router (“mrouter”). Click **IP Application > DVMRP** in the navigation panel to display the screen as shown.

Figure 174 IP Application > DVMRP

DVMRP

Active ☐

Threshold

Index	Network	VID	Active
1	10.10.10.1/24	2	☐
2	192.168.1.1/24	1	☐

The following table describes the labels in this screen.

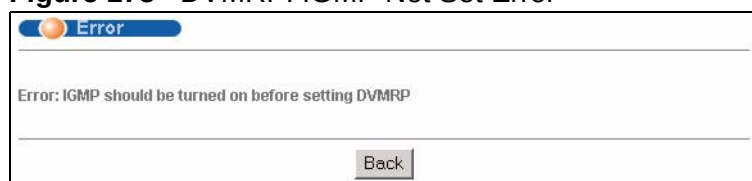
Table 124 IP Application > DVMRP

LABEL	DESCRIPTION
Active	Select Active to enable DVMRP on the Switch. You should do this if you want the Switch to act as a multicast router.
Threshold	Threshold is the maximum time to live (TTL) value. TTL is used to limit the scope of multicasting. You should reduce this value if you do not wish to flood Layer-3 devices many hops away with multicast traffic. This applies only to multicast traffic this Switch sends out.
Index	Index is the DVMRP configuration for the IP routing domain defined under Network . The maximum number of DVMRP configurations allowed is the maximum number of IP routing domains allowed on the Switch. See Section 8.6 on page 110 for more information on IP routing domains.
Network	This is the IP routing domain IP address and subnet mask you set up in IP Setup .
VID	DVMRP cannot be enabled on the same VLAN group across different IP routing domains, that is, you cannot have duplicate VIDs for different DVMRP configurations (see Figure 177 on page 352).
Active	Select Active to enable DVMRP on this IP routing domain.
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.

39.3.1 DVMRP Configuration Error Messages

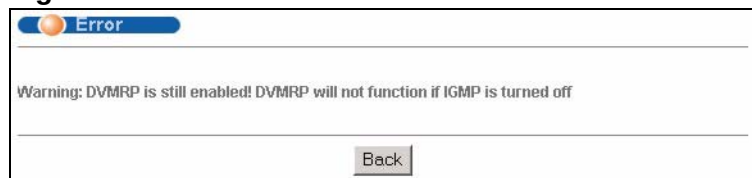
You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in the next figure.

Figure 175 DVMRP: IGMP Not Set Error



When you disable IGMP, but DVMRP is still active you also see another warning screen.

Figure 176 DVMRP: Unable to Disable IGMP Error



Each IP routing domain DVMRP configuration must be in a different VLAN group; otherwise you see the following screen.

Figure 177 DVMRP: Duplicate VID Error Message



39.4 Default DVMRP Timer Values

The following are some default DVMRP timer values.

Table 125 DVMRP: Default Timer Values

DVMRP FIELD	DEFAULT VALUE
Probe interval	10 sec
Report interval	35 sec
Route expiration time	140 sec
Prune lifetime	Variable (less than two hours)
Prune retransmission time	3 sec with exponential back off
Graft retransmission time	5 sec with exponential back off

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

40.1 DiffServ Overview

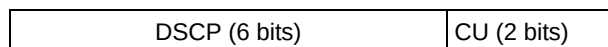
Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

40.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Figure 178 DiffServ: Differentiated Service Field



DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

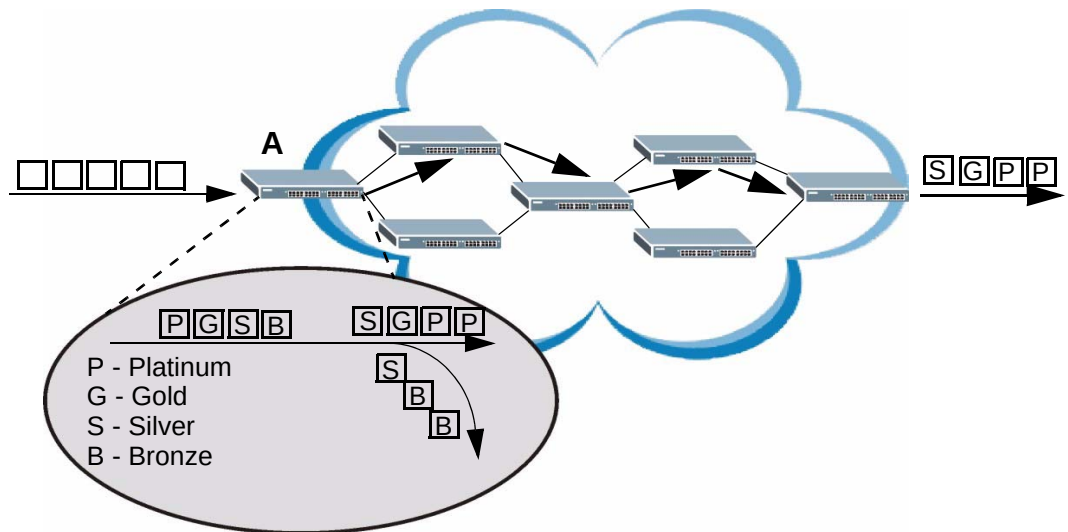
The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different

kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

40.1.2 DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in [Figure 179](#)) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. For example, one traffic policy would be to give higher drop precedence to one traffic flow over others. In our example packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 179 DiffServ Network



40.2 Two Rate Three Color Marker Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.

Two Rate Three Color Marker (TRTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR

specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

Two Rate Three Color Marker evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green. After TRTCM is configured and DiffServ is enabled the following actions are performed on the colored packets:

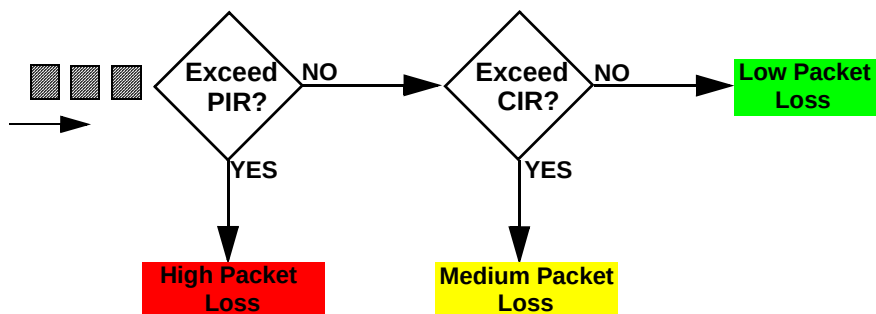
- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.
- Green (low loss priority level) packets are forwarded.

TRTCM operates in one of two modes: color-blind or color-aware. In color-blind mode, packets are marked based on evaluating against the PIR and CIR regardless of if they have previously been marked or not. In the color-aware mode, packets are marked based on both existing color and evaluation against the PIR and CIR. If the packets do not match any of colors, then the packets proceed unchanged.

40.2.1 TRTCM - Color-blind Mode

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

Figure 180 TRTCM - Color-blind Mode



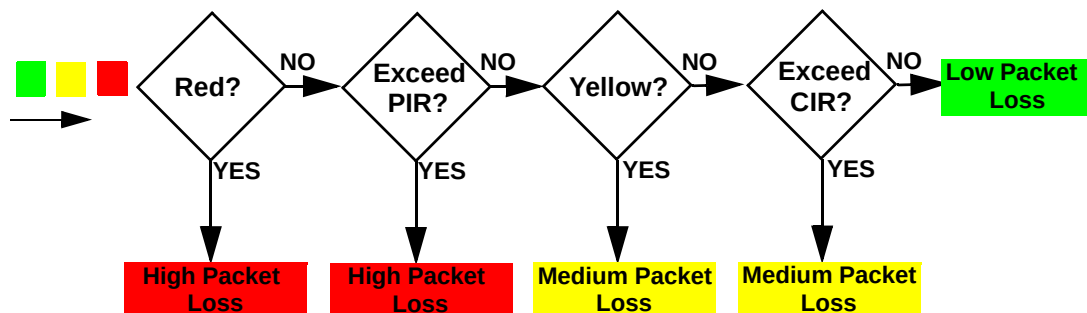
40.2.2 TRTCM - Color-aware Mode

In color-aware mode the evaluation of the packets uses the existing packet loss priority. TRTCM can increase a packet loss priority of a packet but it cannot

decrease it. Packets that have been previously marked red or yellow can only be marked with an equal or higher packet loss priority.

Packets marked red (high packet loss priority) continue to be red without evaluation against the PIR or CIR. Packets marked yellow can only be marked red or remain yellow so they are only evaluated against the PIR. Only the packets marked green are first evaluated against the PIR and then if they don't exceed the PIR level are they evaluated against the CIR.

Figure 181 TRTCM - Color-aware Mode



40.3 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected port(s).

Click **IP Application > DiffServ** in the navigation panel to display the screen as shown.

Figure 182 IP Application > DiffServ

The screenshot shows the 'Diffserv' configuration window. At the top, there are tabs for '2-rate 3 Color Marker' and 'DSCP Setting'. Below the tabs, there is an 'Active' checkbox. The main area contains a table with two columns: 'Port' and 'Active'. The 'Port' column lists ports from 1 to 8, with a '*' symbol above them. The 'Active' column contains checkboxes for each port. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

Port	Active
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐

The following table describes the labels in this screen.

Table 126 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. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select Active to enable DiffServ on the port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

40.3.1 Configuring 2-Rate 3 Color Marker Settings

Use this screen to configure TRTCM settings. Click the **2-rate 3 Color Marker** link in the **DiffServ** screen to display the screen as shown next.

Note: You cannot enable both TRTCM and Bandwidth Control at the same time.

Figure 183 IP Application > DiffServ > 2-rate 3 Color Marker

Port	Active	Commit Rate	Peak Rate	green	yellow	red
*	☐	Kbps	Kbps			
1	☐	Kbps	Kbps			
2	☐	Kbps	Kbps			
3	☐	Kbps	Kbps			
4	☐	Kbps	Kbps			
5	☐	Kbps	Kbps			
6	☐	Kbps	Kbps			
7	☐	Kbps	Kbps			
8	☐	Kbps	Kbps			

Apply Cancel

The following table describes the labels in this screen.

Table 127 IP Application > DiffServ > 2-rate 3 Color Marker

LABEL	DESCRIPTION
Active	Select this to activate TRTCM (Two Rate Three Color Marker) on the Switch. The Switch evaluates and marks the packets based on the TRTCM settings. Note: You must also activate DiffServ on the Switch and the individual ports for the Switch to drop red (high loss priority) colored packets.
Mode	Select color-blind to have the Switch treat all incoming packets as uncolored. All incoming packets are evaluated against the CIR and PIR. Select color-aware to treat the packets as marked by some preceding entity. Incoming packets are evaluated based on their existing color. Incoming packets that are not marked proceed through the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to activate TRTCM on the port.

Table 127 IP Application > DiffServ > 2-rate 3 Color Marker (continued)

LABEL	DESCRIPTION
Commit Rate	Specify the Commit Information Rate (CIR) for this port.
Peak Rate	Specify the Peak Information Rate (PIR) for this port.
DSCP	Use this section to specify the DSCP values that you want to assign to packets based on the color they are marked via TRTCM.
green	Specify the DSCP value to use for packets with low packet loss priority.
yellow	Specify the DSCP value to use for packets with medium packet loss priority.
red	Specify the DSCP value to use for packets with high packet loss priority.
Apply	Click 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.

40.4 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

Table 128 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

40.4.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping, click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 184 IP Application > DiffServ > DSCP Setting

The screenshot shows the 'DSCP Setting' screen with a 'DSCP to 802.1p Mapping' table. The table has 64 rows, each with a DSCP value (0-63) and a corresponding 802.1p priority (0-7). The mapping is as follows:

DSCP	802.1p
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	2
17	2
18	2
19	2
20	2
21	2
22	2
23	2
24	3
25	3
26	3
27	3
28	3
29	3
30	3
31	3
32	4
33	4
34	4
35	4
36	4
37	4
38	4
39	4
40	5
41	5
42	5
43	5
44	5
45	5
46	5
47	5
48	6
49	6
50	6
51	6
52	6
53	6
54	6
55	6
56	7
57	7
58	7
59	7
60	7
61	7
62	7
63	7

At the bottom of the screen are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 129 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.

This chapter shows you how to configure the DHCP feature.

41.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the Switch as a DHCP server or a DHCP relay agent. When configured as a server, the Switch provides the TCP/IP configuration for the clients. If you configure the Switch as a relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a DHCP server or relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

41.1.1 DHCP Modes

The Switch can be configured as a DHCP server or DHCP relay agent.

- If you configure the Switch as a DHCP server, it will maintain the pool of IP addresses along with subnet masks, DNS server and default gateway information and distribute them to your LAN computers.
- If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

41.1.2 DHCP Configuration Options

The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The Switch forwards all DHCP requests to the same DHCP server.

- **VLAN** - The Switch is configured on a VLAN by VLAN basis. The Switch can be configured as a DHCP server for one VLAN and at the same time the Switch can be configured to relay DHCP requests for clients in another VLAN.

41.2 DHCP Status

Click **IP Application > DHCP** in the navigation panel. The **DHCP Status** screen displays.

Figure 185 IP Application > DHCP Status

DHCP Status			
Global			
VLAN			
Server Status:			
Index	VID	Server Status	IP Pool Size
1	2	192.168.2.100	66
Relay Status			
Relay Mode		VLAN:1-3	

The following table describes the labels in this screen.

Table 130 IP Application > DHCP Status

LABEL	DESCRIPTION
Server Status	This section displays configuration settings related to the Switch's DHCP server mode.
Index	This is the index number.
VID	This field displays the VLAN ID for which the Switch is a DHCP server.
Server Status	This field displays the starting DHCP client IP address.
IP Pool Size	This field displays the number of IP addresses that can be assigned to clients.
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: • None - if the Switch is not configured as a DHCP relay agent. • Global - if the Switch is configured as a DHCP relay agent only. • VLAN - followed by a VLAN ID if it is configured as a relay agent for specific VLAN(s).

41.3 DHCP Server Status Detail

Click **IP Application > DHCP** in the navigation panel and then click an existing index number of a DHCP server configuration to view the screen as shown. Use

this screen to view details regarding DHCP server settings configured on the Switch.

Figure 186 IP Application > DHCP > DHCP Server Status Detail

Server Status Detail

DHCP Status

Start IP Address	192.168.1.33
End IP Address	192.168.1.62
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Primary DNS Server	192.168.5.1
Secondary DNS Server	192.168.5.2

Address Leases

Index	IP Address	Timer	Hardware Address	Hostname

The following table describes the labels in this screen.

Table 131 IP Application > DHCP Server Status Detail

LABEL	DESCRIPTION
Start IP Address	This field displays the starting IP address of the IP address pool configured for this DHCP server instance.
End IP Address	This field displays the last IP address of the IP address pool configured for this DHCP server instance.
Subnet Mask	This field displays the subnet mask value sent to clients from this DHCP server instance.
Default Gateway	This field displays the default gateway value sent to clients from this DHCP server instance.
Primary DNS Server	This field displays the primary DNS server value sent to clients from this DHCP server instance.
Secondary DNS Server	This field displays the secondary DNS server value sent to clients from this DHCP server instance.
Address Leases	This section displays information about the IP addresses this DHCP server issued to clients.
Index	This field displays a sequential number for each DHCP request handled by the Switch.
IP Address	This is the IP address issued to a DHCP client.
Timer	This field displays the time remaining before the DHCP client has to renew its IP address.
Hardware Address	This field displays the MAC address of the DHCP client. It may also display SELF OCCUPIED ADDRESS if the IP address cannot be used for DHCP because it is already assigned to the Switch itself.
Hostname	This field displays the system name of the client.

41.4 DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

41.4.1 DHCP Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. 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 Settings > General Setup**.

The following describes the DHCP relay information that the Switch sends to the DHCP server:

Table 132 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 .

41.4.2 Configuring DHCP Global Relay

Configure global DHCP relay in the **DHCP Relay** screen. Click **IP Application > DHCP** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 187 IP Application > DHCP > Global

The following table describes the labels in this screen.

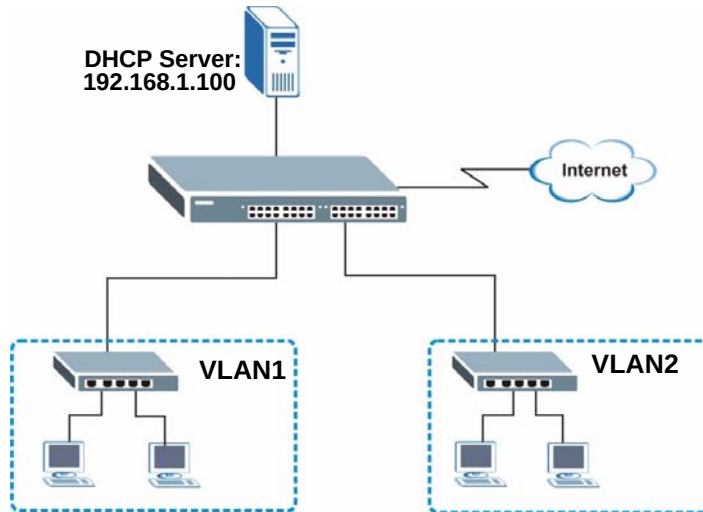
Table 133 IP Application > DHCP > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the Option 82 check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the General Setup screen. Select the check box for the Switch to add the system name to the client 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.

41.4.3 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 188 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 189 DHCP Relay Configuration Example

The screenshot shows the DHCP Relay configuration interface. The 'Active' checkbox is checked. The 'Remote DHCP Server 1' is set to 192.168.1.100. The 'Remote DHCP Server 2' and 'Remote DHCP Server 3' are both set to 0.0.0.0. The 'Relay Agent Information' section has the 'Option 82' checkbox checked. The 'Information' checkbox is unchecked. At the bottom, there are 'Apply' and 'Cancel' buttons, and a red 'EXAMPLE' label.

DHCP Relay		Status
Active	☒	
Remote DHCP Server 1	192.168.1.100	
Remote DHCP Server 2	0.0.0.0	
Remote DHCP Server 3	0.0.0.0	
Relay Agent Information	☒ Option 82	
Information	☐	

Apply Cancel **EXAMPLE**

41.5 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application > DHCP** in the navigation panel, then click the **VLAN** link In the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch. See [Section 8.6 on page 110](#) for information on how to do this.

Figure 190 IP Application > DHCP > VLAN

VLAN Setting Status

VID:

DHCP Status: ☒ Server ☐ Relay

Server

Client IP Pool Starting Address:

Size of Client IP Pool:

IP Subnet Mask:

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

Relay

Remote DHCP Server 1:

Remote DHCP Server 2:

Remote DHCP Server 3:

Relay Agent Information: ☐ Option 82

Information: ☐

VID	Type	DHCP Status	Delete
2	Server	192.168.2.100/66	☐

The following table describes the labels in this screen.

Table 134 IP Application > DHCP > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
DHCP Status	Select whether the Switch should function as a DHCP Server or Relay for the specified VID. If you select Server then fields related to DHCP relay configuration are grayed out and vice versa.

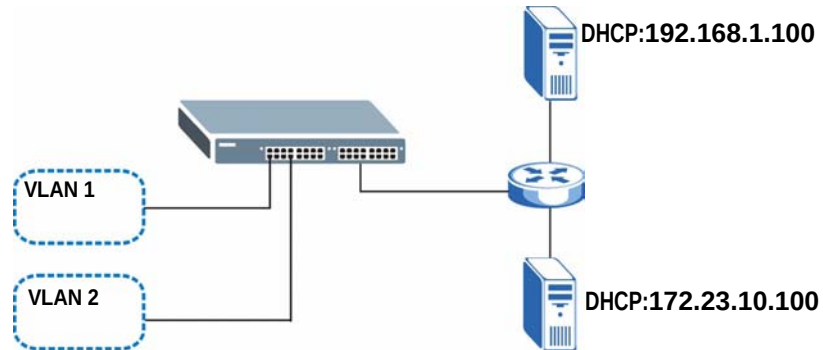
Table 134 IP Application > DHCP > VLAN (continued)

LABEL	DESCRIPTION
Server	Use this section if you want to configure the Switch to function as a DHCP server for this VLAN.
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool. The Switch can issue from 1 to 253 IP addresses to DHCP clients.
IP Subnet Mask	Enter the subnet mask for the client IP pool.
Default Gateway	Enter the IP address of the default gateway device.
Primary/Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Relay	Use this section if you want to configure the Switch to function as a DHCP relay for this VLAN.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the Option 82 check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the General Setup screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
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 this to clear the fields above.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays Server or Relay for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click Delete to remove them.
Cancel	Click Cancel to clear the Delete check boxes.

41.5.1 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 172.23.10.100.

Figure 191 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 192 DHCP Relay for Two VLANs Configuration Example

The screenshot shows the 'VLAN Setting' configuration interface. At the top, there's a 'VLAN Setting' header with a status indicator. Below it, the 'VID' is set to 2. The 'DHCP Status' is set to 'Relay' (selected with a radio button). Under the 'Server' section, fields for 'Client IP Pool Starting Address', 'Size of Client IP Pool', 'IP Subnet Mask', 'Default Gateway', 'Primary DNS Server', and 'Secondary DNS Server' are all set to 0.0.0.0. Under the 'Relay' section, 'Remote DHCP Server 1' is set to 172.23.10.100, while 'Remote DHCP Server 2' and 'Remote DHCP Server 3' are set to 0.0.0.0. There are checkboxes for 'Relay Agent Information' and 'Option 82', both of which are unchecked. Below the configuration fields are 'Add', 'Cancel', and 'Clear' buttons. At the bottom, there is a table listing the configured VLANs.

VID	Type	DHCP Status	Delete
1	Relay	192.168.1.100	☐

Below the table are 'Delete' and 'Cancel' buttons. A red 'EXAMPLE' label is present in the bottom right corner of the interface.

This chapter shows you how to configure and monitor the Virtual Router Redundancy Protocol (VRRP) on the Switch.

42.1 VRRP Overview

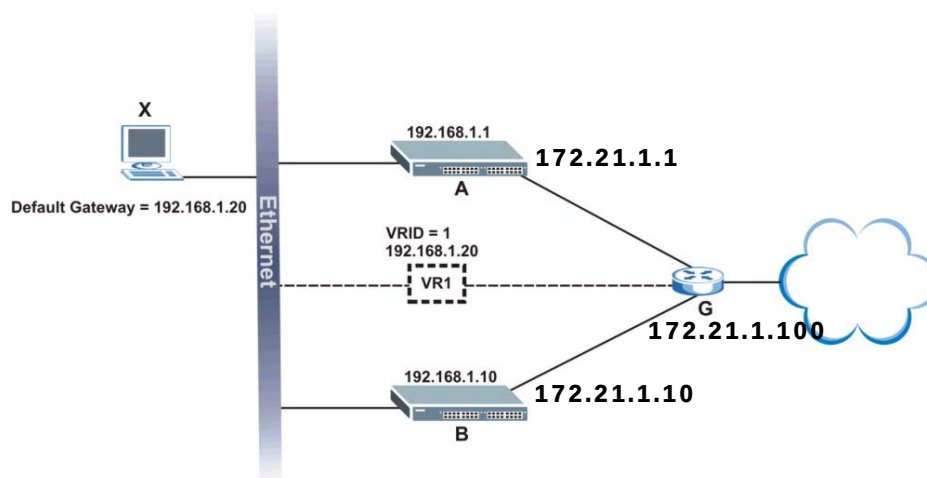
Each host on a network is configured to send packets to a statically configured default gateway (this Switch). The default gateway can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

In VRRP, a virtual router (VR) represents a number of physical layer-3 devices. An IP address is associated with the virtual router. A layer-3 device having the same IP address is the preferred master router while the other Layer-3 devices are the backup routers. The master router forwards traffic for the virtual router. When the master router becomes unavailable, a backup router assumes the role of the master router until the master router comes back up and takes over.

The following figure shows a VRRP network example with the switches (**A** and **B**) implementing one virtual router **VR1** to ensure the link between the host **X** and the uplink gateway **G**. Host **X** is configured to use **VR1** (192.168.1.20) as the

default gateway. If switch **A** has a higher priority, it is the master router. Switch **B**, having a lower priority, is the backup router.

Figure 193 VRRP: Example 1



If switch **A** (the master router) is unavailable, switch **B** takes over. Traffic is then processed by switch **B**.

42.2 VRRP Status

Click **IP Application > VRRP** in the navigation panel to display the **VRRP Status** screen as shown next.

Figure 194 IP Application > VRRP Status

VRRP Status				Configuration
Index	Network	VRID	VR Status	Uplink Status
1	192.168.1.1/24	1	Master	Alive
Poll Interval(s) 10 Set Interval Stop				

The following table describes the labels in this screen.

Table 135 IP Application > VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Network	This field displays the IP address and the subnet mask bits of an IP routing domain that is associated to a virtual router.
VRID	This field displays the ID number of the virtual router.

Table 135 IP Application > VRRP Status (continued)

LABEL	DESCRIPTION
VR Status	This field displays the status of the virtual router. This field is Master indicating that this Switch functions as the master router. This field is Backup indicating that this Switch functions as a backup router. This field displays Init when this Switch is initiating the VRRP protocol or when the Uplink Status field displays Dead.
Uplink Status	This field displays the status of the link between this Switch and the uplink gateway. This field is Alive indicating that the link between this Switch and the uplink gateway is up. Otherwise, this field is Dead. This field displays Probe when this Switch is check for the link state.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval.
Stop	Click Stop to halt system statistic polling.

42.3 VRRP Configuration

The following sections describe the different parts of the VRRP Configuration screen.

42.3.1 IP Interface Setup

Before configuring VRRP, first create an IP interface (or routing domain) in the **IP Setup** screen (see the [Section 8.6 on page 110](#) for more information).

Click **IP Application**, **VRRP** and click the **Configuration** link to display the **VRRP Configuration** screen as shown next.

Note: You can only configure VRRP on interfaces with unique VLAN IDs.

Note: Routing domains with the same VLAN ID are not displayed in the table indicated.

Figure 195 IP Application > VRRP Configuration > IP Interface

VRRP Configuration Status

Index	Network	Authentication	Key
1	192.168.1.10/24	None	

Apply Cancel

Active ☐

Name

Network

Virtual Router ID

Advertisement Interval

Preempt Mode ☒

Priority

Uplink Gateway

Primary Virtual IP

Secondary Virtual IP

Add Cancel Clear

Index	Active	Name	Network	VRID	Primary VIP	Uplink Gateway	Priority	Delete
1	Yes	Example	192.168.1.10/24	1	192.168.1.1	192.168.1.100	110	☐

Delete Cancel

The following table describes the labels in this screen.

Table 136 IP Application > VRRP Configuration > IP Interface

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Network	This field displays the IP address and number of subnet mask bit of an IP domain.
Authentication	Select None to disable authentication. This is the default setting. Select Simple to use a simple password to authenticate VRRP packet exchanges on this interface.
Key	When you select Simple in the Authentication field, enter a password key (up to eight printable ASCII character long) in this field.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to discard all changes made in this table.

42.3.2 VRRP Parameters

This section describes the VRRP parameters.

42.3.2.1 Advertisement Interval

The master router sends out Hello messages to let the other backup routers know that it is still up and running. The time interval between sending the Hello messages is the advertisement interval. By default, a Hello message is sent out every second.

If the backup routers do not receive a Hello message from the master router after this interval expires, it is assumed that the master router is down. Then the backup router with the highest priority becomes the master router.

Note: All routers participating in the virtual router must use the same advertisement interval.

42.3.2.2 Priority

Configure the priority level (1 to 254) to set which backup router to take over in case the master router goes down. The backup router with the highest priority will take over. The priority of the VRRP router that owns the IP address(es) associated with the virtual router is 255.

42.3.2.3 Preempt Mode

If the master router is unavailable, a backup router assumes the role of the master router. However, when another backup router with a higher priority joins the network, it will preempt the lower priority backup router that is the master. Disable preempt mode to prevent this from happening.

By default, a layer 3 device with the same IP address as the virtual router will become the master router regardless of the preempt mode.

42.3.3 Configuring VRRP Parameters

After you set up an IP interface, configure the VRRP parameters in the **VRRP Configuration** screen.

Figure 196 IP Application > VRRP Configuration > VRRP Parameters

The following table describes the labels in this screen.

Table 137 IP Application > VRRP Configuration > VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Network	Select an IP domain to which this VRRP entry applies.
Virtual Router ID	Select a virtual router number (1 to 7) for which this VRRP entry is created. You can configure up to seven virtual routers for one network.
Advertisement Interval	Specify the number of seconds between Hello message transmissions. The default is 1 .
Preempt Mode	Select this option to activate preempt mode.
Priority	Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority. This field is 100 by default.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The Switch checks the link to the uplink gateway.
Primary Virtual IP	Enter the IP address of the primary virtual router in dotted decimal notation.
Secondary Virtual IP	This field is optional. Enter the IP address of a secondary virtual router in dotted decimal notation. This field is ignored when you enter 0.0.0.0 .

Table 137 IP Application > VRRP Configuration > VRRP Parameters (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 discard all changes made in this table.
Clear	Click Clear to set the above fields back to the factory defaults.

42.3.4 Configuring VRRP Parameters

View the VRRP configuration summary at the bottom of the screen.

Figure 197 VRRP Configuration: Summary

Index	Active	Name	Network	VRID	Primary VIP	Uplink Gateway	Priority	Delete
1	Yes	Example	192.168.1.10/24	1	192.168.1.1	192.168.1.100	110	☐

The following table describes the labels in this screen.

Table 138 VRRP Configuring: VRRP Parameters

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Active	This field shows whether a VRRP entry is enabled (Yes) or disabled (No).
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and subnet mask of an interface.
VRID	This field displays the ID number of a virtual router.
Primary VIP	This field displays the IP address of the primary virtual router.
Uplink Gateway	This field displays the IP address of the uplink gateway.
Priority	This field displays the priority level (1 to 255) of the entry.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

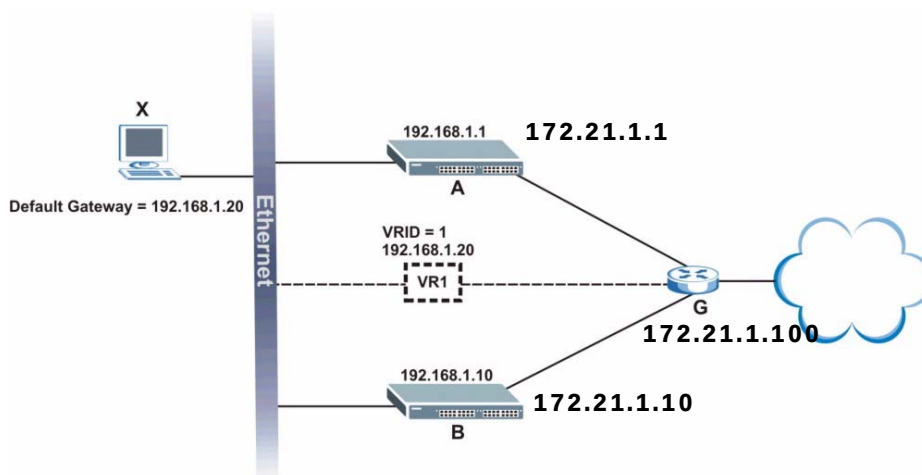
42.4 VRRP Configuration Examples

The following sections show two VRRP configuration examples on the Switch.

42.4.1 One Subnet Network Example

The figure below shows a simple VRRP network with only one virtual router **VR1** (VRID =1) and two switches. The network is connected to the WAN via an uplink gateway **G** (172.21.1.100). The host computer **X** is set to use **VR1** as the default gateway.

Figure 198 VRRP Configuration Example: One Virtual Router Network



You want to set switch **A** as the master router. Configure the VRRP parameters in the **VRRP Configuration** screens on the switches as shown in the figures below.

Figure 199 VRRP Example 1: VRRP Parameter Settings on Switch A

Active	☒
Name	Example1
Network	192.168.1.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	☒
Priority	110
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

EXAMPLE

Figure 200 VRRP Example 1: VRRP Parameter Settings on Switch B

Active	☒
Name	Example1
Network	192.168.1.10/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	☒
Priority	100
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

EXAMPLE

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 201 VRRP Example 1: VRRP Status on Switch A

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.1/24	1	Master	Alive

EXAMPLE

Figure 202 VRRP Example 1: VRRP Status on Switch B

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.10/24	1	Backup	Alive

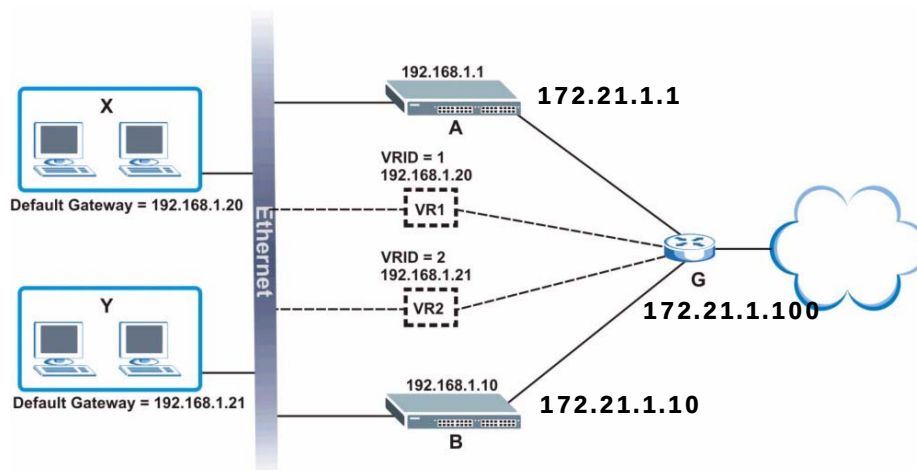
EXAMPLE

42.4.2 Two Subnets Example

The following figure depicts an example in which two switches share the network traffic. Hosts in the two network groups use different default gateways. Each switch is configured to backup a virtual router using VRRP.

You wish to configure switch **A** as the master router for virtual router **VR1** and as a backup for virtual router **VR2**. On the other hand, switch **B** is the master for **VR2** and a backup for **VR1**.

Figure 203 VRRP Configuration Example: Two Virtual Router Network



You need to configure the **VRRP Configuration** screen for virtual router VR2 on each switch, while keeping the VRRP configuration in example 1 for virtual router

VR1 (refer to [Section 42.4.2 on page 379](#)). Configure the VRRP parameters on the switches as shown in the figures below.

Figure 204 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A

Active	☒
Name	Example2
Network	192.168.1.1/24
Virtual Router ID	2
Advertisement Interval	1
Preempt Mode	☒
Priority	100
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

EXAMPLE

Figure 205 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B

Active	☒
Name	Example2
Network	192.168.1.10/24
Virtual Router ID	2
Advertisement Interval	1
Preempt Mode	☒
Priority	110
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

EXAMPLE

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 206 VRRP Example 2: VRRP Status on Switch A

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.1/24	2	Backup	Alive
2	Yes	192.168.1.1/24	1	Master	Alive

EXAMPLE

Figure 207 VRRP Example 2: VRRP Status on Switch B

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.10/24	2	Master	Alive
2	Yes	192.168.1.10/24	1	Backup	Alive

EXAMPLE

ARP Learning

43.1 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.

43.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

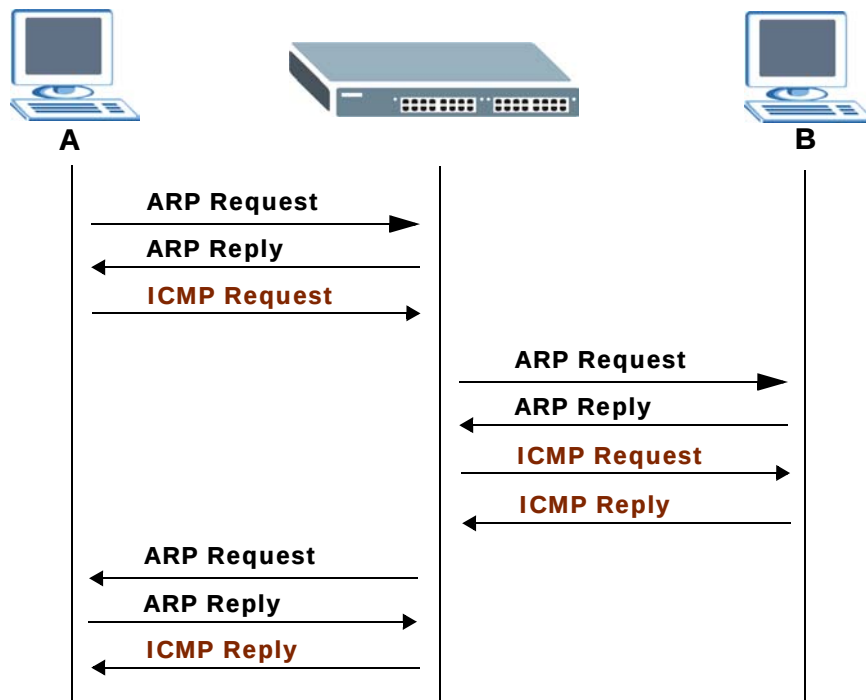
43.1.2 ARP Learning Mode

The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

43.1.2.1 ARP-Reply

By default, the Switch is in ARP-Reply learning mode and 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**.



43.1.2.2 Gratuitous-ARP

A gratuitous ARP is an ARP request in which both the source and destination IP address fields are set to the IP address of the device that sends this request and the destination MAC address field is set to the broadcast address. There will be no reply to a gratuitous ARP request.

A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform

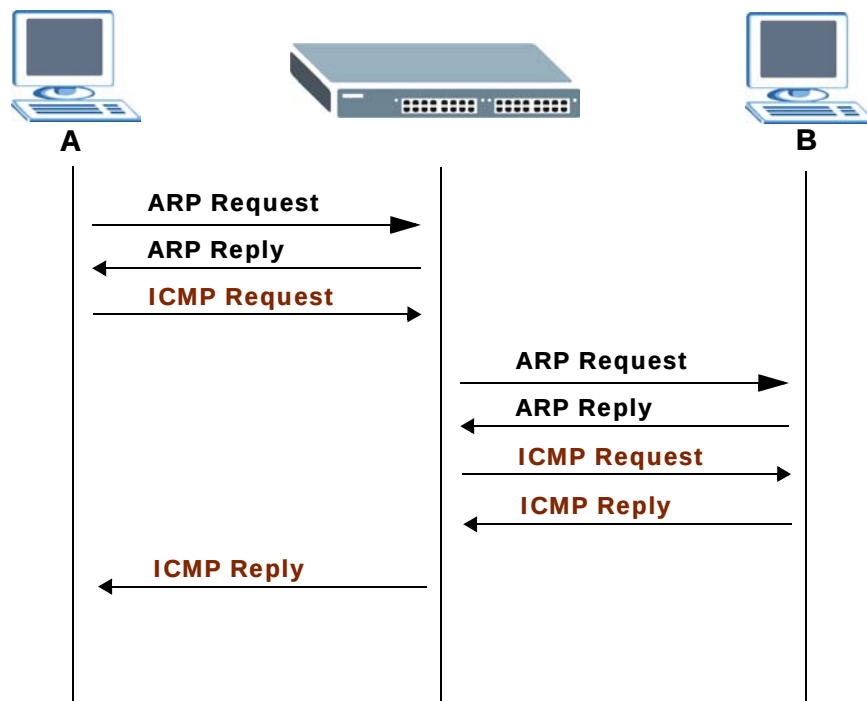
other devices in the same network to update their ARP table with the new mapping information.

In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

43.1.2.3 ARP-Request

When the Switch is in ARP-Request learning mode, it updates the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.

Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



43.2 Configuring ARP Learning

Click **IP Application > ARP Learning** in the navigation panel to display the screen as shown next.

Figure 208 IP Application > ARP Learning

Port	ARP Learning Mode
*	ARP-Reply
1	ARP-Reply
2	ARP-Reply
3	ARP-Reply
4	ARP-Reply
5	ARP-Reply
6	ARP-Reply
7	ARP-Reply
8	ARP-Reply
9	ARP-Reply
10	ARP-Reply
11	ARP-Reply

Apply Cancel

The following table describes the labels in this screen.

Table 139 IP Application > 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. Note: Changes in this row are copied to all the ports as soon as you make them.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select ARP-Reply to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select Gratuitous-ARP to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select ARP-Request to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.

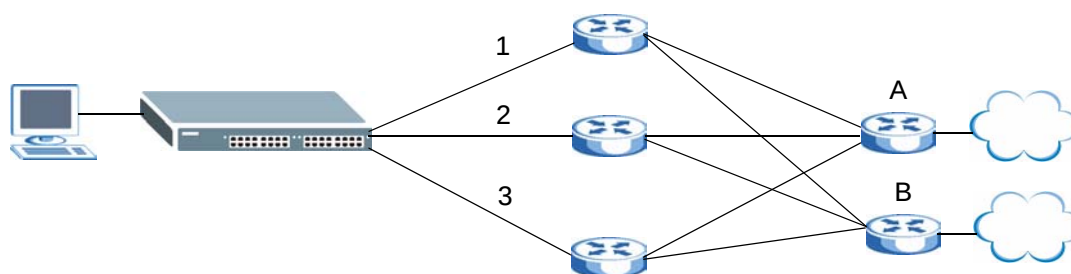
Table 139 IP Application > ARP Learning (continued)

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.

Load Sharing

44.1 Load Sharing Overview

The Switch learns the next-hop(s) using ARP and determines routing path(s) for a destination. The Switch supports Equal-Cost MultiPath (ECMP) to forward packets destined to the same device (**A** for example) through different routing paths (**1**, **2** and **3**) of equal path cost. This allows you to balance or share traffic loads between multiple routing paths when the Switch is connected to more than one next-hop. ECMP works with static routes or a routing protocol, such as OSPF.



With ECMP, packets are routed through the paths of equal cost according to the hash algorithm output.

44.2 Configuring Load Sharing

Click **IP Application > Load Sharing** in the navigation panel to display the screen as shown next.

Figure 209 IP Application > Load Sharing

Load Sharing	
Active	☐
Criteria	src-dst-ip
Aging Time	1200 seconds
Discover Time	3600 seconds
Apply Cancel	

The following table describes the labels in this screen.

Table 140 IP Application > Load Sharing

LABEL	DESCRIPTION
Active	Select this option to enable Equal-Cost MultiPath (ECMP) routing on the Switch.
Criteria	Select the criteria the Switch uses to determine the routing path for a packet. Select src-ip to have the Switch use a hash algorithm to convert a packet's source IP address into a hash value which acts as an index to a route path. Select src-dst-ip to have the Switch use a hash algorithm to convert a packet's source and destination IP addresses into a hash value which acts as an index to a route path.
Aging Time	Specify the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update a resolved next-hop's MAC address.
Discover Time	Specify the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update an unresolved next-hop's MAC address.
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.

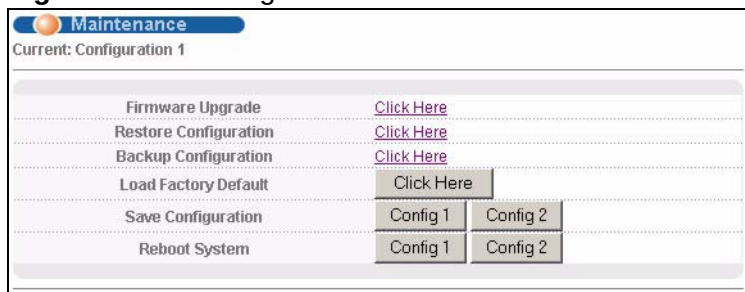
Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

45.1 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management > Maintenance** in the navigation panel to open the following screen.

Figure 210 Management > Maintenance



The following table describes the labels in this screen.

Table 141 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (Configuration 1 or Configuration 2) is currently operating on the Switch.
Firmware Upgrade	Click Click Here to go to the Firmware Upgrade screen.
Restore Configuration	Click Click Here to go to the Restore Configuration screen.
Backup Configuration	Click Click Here to go to the Backup Configuration screen.
Load Factory Default	Click Click Here to reset the configuration to the factory default settings.

Table 141 Management > Maintenance (continued)

LABEL	DESCRIPTION
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.
Reboot System	Click Config 1 to reboot the system and load Configuration 1 on the Switch. Click Config 2 to reboot the system and load Configuration 2 on the Switch. Note: Make sure to click the Save button in any screen to save your settings to the current configuration on the Switch.

45.2 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Default** to clear all Switch configuration information you configured and return to the factory defaults.
- 2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 211 Load Factory Default: Start

- 3 In the web configurator, click the **Save** button 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).

45.3 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

45.4 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

- 1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 212 Reboot System: Confirmation



- 2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

45.5 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

Figure 213 Management > Maintenance > Firmware Upgrade

Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Select the **Rebooting** checkbox if you want to reboot the Switch and apply the new firmware immediately. (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

45.6 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 214 Management > Maintenance > Restore Configuration

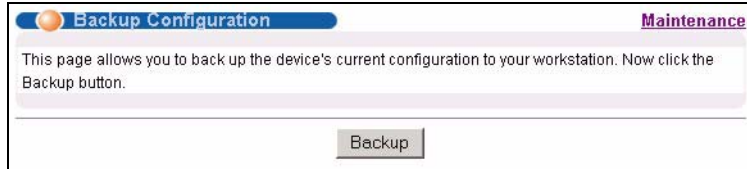
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

45.7 Backup a Configuration File

Backing up your Switch configurations allows you to create various “snapshots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 215 Management > Maintenance > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

- 1 Click **Backup**.
- 2 Click **Save** to display the **Save As** screen.
- 3 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.

45.8 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

45.8.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System, sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension.

Table 142 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	.cfg	This is the configuration (config) filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

45.8.1.1 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.

45.8.2 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter open, followed by a space and the IP address of your Switch.
- 3 Press [ENTER] when prompted for a username (the default is “admin”).
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter bin to set transfer mode to binary.

- 6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` 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 142 on page 394](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

45.8.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 143 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).

45.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

Access Control

This chapter describes how to control access to the Switch.

46.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 144 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the Ethernet Switch CLI Reference Guide for more information on disabling multi-login.

46.2 The Access Control Main Screen

Click **Management > Access Control** in the navigation panel to display the main screen as shown.

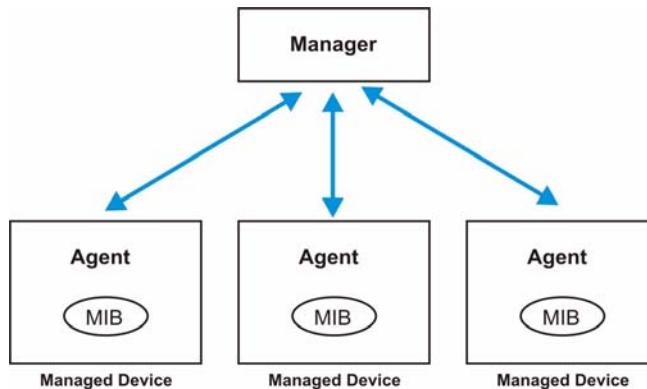
Figure 216 Management > Access Control



46.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version one (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 217 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a Switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 145 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

46.3.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

46.3.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

46.3.3 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with “**1.3.6.1.4.1.890.1.5.8**” is defined in private MIBs. Otherwise, it is a standard MIB OID.

The OIDs beginning with “**1.3.6.1.4.1.890.1.5.8.52**” are specific to the XGS-4526 switch.

The OIDs beginning with “**1.3.6.1.4.1.890.1.5.8.39**” are specific to the XGS-4528F switch.

The OIDs beginning with “**1.3.6.1.4.1.890.1.5.8.46**” are specific to the XGS-4728F switch.

Table 146 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	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.8.52.3 1.2.2 1.3.6.1.4.1.890.1.5.8.39.3 1.2.2 1.3.6.1.4.1.890.1.5.8.46.3 1.2.2	This trap is sent when the fan speed returns to the normal operating range.

Table 146 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.8.52.3 1.2.2 1.3.6.1.4.1.890.1.5.8.39.3 1.2.2 1.3.6.1.4.1.890.1.5.8.46.3 1.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.8.52.3 1.2.2 1.3.6.1.4.1.890.1.5.8.39.3 1.2.2 1.3.6.1.4.1.890.1.5.8.46.3 1.2.2	This trap is sent when the voltage returns to the normal operating range.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when the Switch automatically resets.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when the Switch resets by an administrator through a management interface.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.

Table 146 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
timesync	RTCNotUpdatedEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when the Switch fails to get the time and date from a time server.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.8.52.3 1.2.2 1.3.6.1.4.1.890.1.5.8.39.3 1.2.2 1.3.6.1.4.1.890.1.5.8.46.3 1.2.2	This trap is sent when the Switch gets the time and date from a time server.
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when intrusion lock occurs on a port.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when loopguard shuts down a port.
errdisable	errdisableDetect	1.3.6.1.4.1.890.1.5.8.52.1 30.4.1 1.3.6.1.4.1.890.1.5.8.39.1 30.4.1 1.3.6.1.4.1.890.1.5.8.46.1 30.4.1	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.
	errdisableRecovery	1.3.6.1.4.1.890.1.5.8.52.1 30.4.2 1.3.6.1.4.1.890.1.5.8.39.1 30.4.2 1.3.6.1.4.1.890.1.5.8.46.1 30.4.2	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 147 SNMP InterfaceTraps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.8.52.31.2.2 1.3.6.1.4.1.890.1.5.8.39.31.2.2 1.3.6.1.4.1.890.1.5.8.46.31.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.8.52.31.2.1 1.3.6.1.4.1.890.1.5.8.39.31.2.1 1.3.6.1.4.1.890.1.5.8.46.31.2.1	This trap is sent when the Ethernet link is down.
autonegotiation	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.8.52.31.2.1 1.3.6.1.4.1.890.1.5.8.39.31.2.1 1.3.6.1.4.1.890.1.5.8.46.31.2.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.8.52.31.2.2 1.3.6.1.4.1.890.1.5.8.39.31.2.2 1.3.6.1.4.1.890.1.5.8.46.31.2.2	This trap is sent when an Ethernet interface auto-negotiates 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 147 SNMP InterfaceTraps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
transceiver-ddm	DDMIRxPowerEventOn	1.3.6.1.4.1.890.1.5.8.52.31.2.1	This trap is sent when one of the device operating parameters (such as transceiver temperature, laser bias current, transmitted optical power, received optical power and transceiver supply voltage) is above or below a factory set normal range.
	DDMITemperatureEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	
	DDMITxBiasEventOn	1.3.6.1.4.1.890.1.5.8.46.31.2.1	
	DDMITxPowerEventOn	1.3.6.1.4.1.890.1.5.8.46.31.2.1	
	DDMIVoltageEventOn	1.3.6.1.4.1.890.1.5.8.46.31.2.1	
	DDMIRxPowerEventClear	1.3.6.1.4.1.890.1.5.8.52.31.2.2	This trap is sent when all device operating parameters return to the normal operating range.
	DDMITemperatureEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	
	DDMITxBiasEventClear	1.3.6.1.4.1.890.1.5.8.46.31.2.2	
	DDMITxPowerEventClear	1.3.6.1.4.1.890.1.5.8.46.31.2.2	
	DDMIVoltageEventClear	1.3.6.1.4.1.890.1.5.8.46.31.2.2	

Table 148 AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.8.52.31.2.1 1.3.6.1.4.1.890.1.5.8.39.31.2.1 1.3.6.1.4.1.890.1.5.8.46.31.2.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.52.31.2.1 1.3.6.1.4.1.890.1.5.8.39.31.2.1 1.3.6.1.4.1.890.1.5.8.46.31.2.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.52.31.2.2 1.3.6.1.4.1.890.1.5.8.39.31.2.2 1.3.6.1.4.1.890.1.5.8.46.31.2.2	This trap is sent when the RADIUS server can be reached.

Table 148 AAA Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
accounting	RADIUSAcctNotReachable EventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1 1.3.6.1.4.1.890.1.5.8.39.3 1.2.1 1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	This trap is sent when there is no response message from the RADIUS accounting server.
	RADIUSAcctNotReachable EventClear	1.3.6.1.4.1.890.1.5.8.52.3 1.2.2 1.3.6.1.4.1.890.1.5.8.39.3 1.2.2 1.3.6.1.4.1.890.1.5.8.46.3 1.2.2	This trap is sent when the RADIUS accounting server can be reached.

Table 149 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 150 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MRSTPNewRoot	1.3.6.1.4.1.890.1.5.8.52.4 2.2.1	This trap is sent when the MRSTP root switch changes.
		1.3.6.1.4.1.890.1.5.8.39.4 2.2.1	
		1.3.6.1.4.1.890.1.5.8.46.4 2.2.1	
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.8.52.1 07.70.1	This trap is sent when the MSTP root switch changes.
		1.3.6.1.4.1.890.1.5.8.39.1 07.70.1	
		1.3.6.1.4.1.890.1.5.8.46.1 07.70.1	
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MRSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.52.4 2.2.2	This trap is sent when the MRSTP topology changes.
		1.3.6.1.4.1.890.1.5.8.39.4 2.2.2	
		1.3.6.1.4.1.890.1.5.8.46.4 2.2.2	
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.52.1 07.70.2	This trap is sent when the MSTP root switch changes.
		1.3.6.1.4.1.890.1.5.8.39.1 07.70.2	
		1.3.6.1.4.1.890.1.5.8.46.1 07.70.2	
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.8.52.3 1.2.1	This trap is sent when more than 99% of the MAC table is used.
		1.3.6.1.4.1.890.1.5.8.39.3 1.2.1	
		1.3.6.1.4.1.890.1.5.8.46.3 1.2.1	
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.8.52.3 1.2.2	This trap is sent when less than 95% of the MAC table is used.
		1.3.6.1.4.1.890.1.5.8.39.3 1.2.2	
		1.3.6.1.4.1.890.1.5.8.46.3 1.2.2	

Table 150 SNMP Switch Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
rmon	RmonRisingAlarm	1.3.6.1.4.1.890.1.5.1.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.4.1.890.1.5.1.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.
cfm	dot1agCfmFaultAlarm	1.3.111.2.802.1.1.8.0.1	The trap is sent when the Switch detects a connectivity fault.

46.3.4 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 218 Management > Access Control > SNMP

The following table describes the labels in this screen.

Table 151 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). Note: SNMP version 2c is backwards compatible with SNMP version 1.

Table 151 Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
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. Note: This username must match an existing account on the Switch (configured in the Management > Access Control > SNMP > User screen).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

46.3.5 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 219 Management > Access Control > SNMP > Trap Group

The following table describes the labels in this screen.

Table 152 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the SNMP Setting screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See Section 46.3.3 on page 400 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

46.3.6 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 220 Management > Access Control > SNMP > User

Index	Username	SecurityLevel	Authentication	Privacy	Group	Delete
1	test	noauth	MD5	DES	readwrite	☐

The following table describes the labels in this screen.

Table 153 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.

Table 153 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. admin - Members of this group can perform all types of system configuration, including the management of administrator accounts. readwrite - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. readonly - Members of this group have read rights only, meaning the user can collect information from the Switch.
Add	Click 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 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.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to begin configuring this screen afresh.

46.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

Note: It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure Switch settings.

Click **Management > Access Control > Logins** to view the screen as shown.

Figure 221 Management > Access Control > Logins

Login	User Name	Password	Retype to confirm
1			
2			
3			
4			

The following table describes the labels in this screen.

Table 154 Management > Access Control > Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.
Old Password	Type the existing system password (1234 is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation

Table 154 Management > Access Control > Logins (continued)

LABEL	DESCRIPTION
Edit Logins	You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see the Ethernet Switch CLI Reference Guide.
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
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.

46.5 SSH Overview

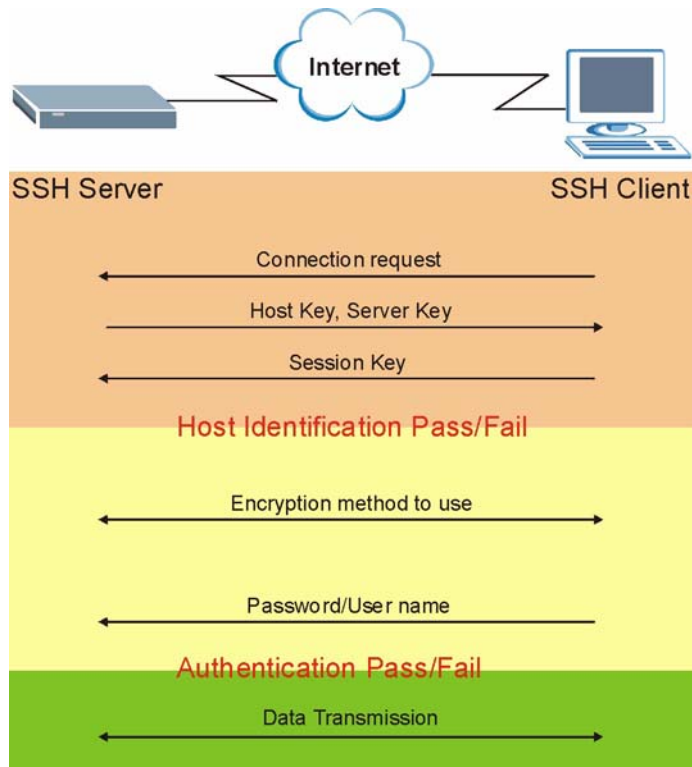
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 222 SSH Communication Example

46.6 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 223 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.

46.7 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

46.7.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

46.8 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

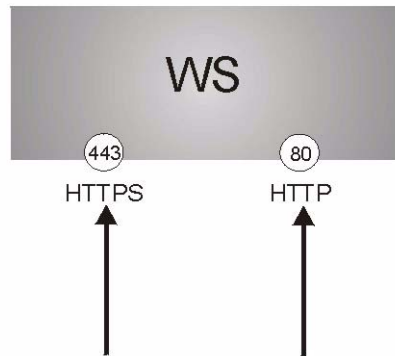
It relies upon certificates, public keys, and private keys.

HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a Certificate Authority (CA) that is a trusted CA on the Switch.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).
- 2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 224 HTTPS Implementation



Note: If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

46.9 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

46.9.1 Internet Explorer Warning Messages

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the Switch.

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 225 Security Alert Dialog Box (Internet Explorer)



46.9.2 Netscape Navigator Warning Messages

When you attempt to access the Switch HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the Switch.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the Switch's certificate into the SSL client.

Figure 226 Security Certificate 1 (Netscape)

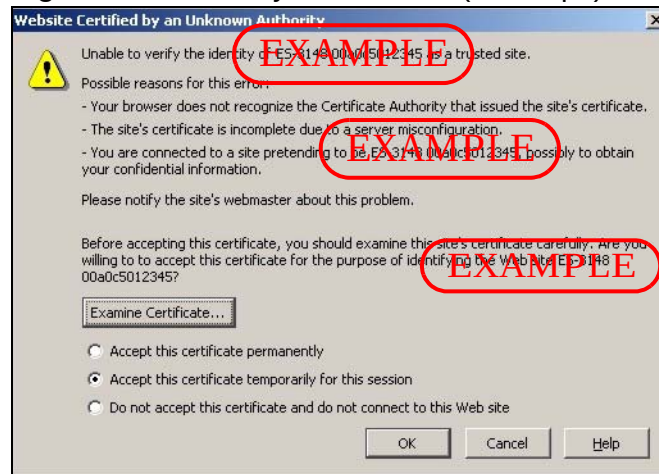


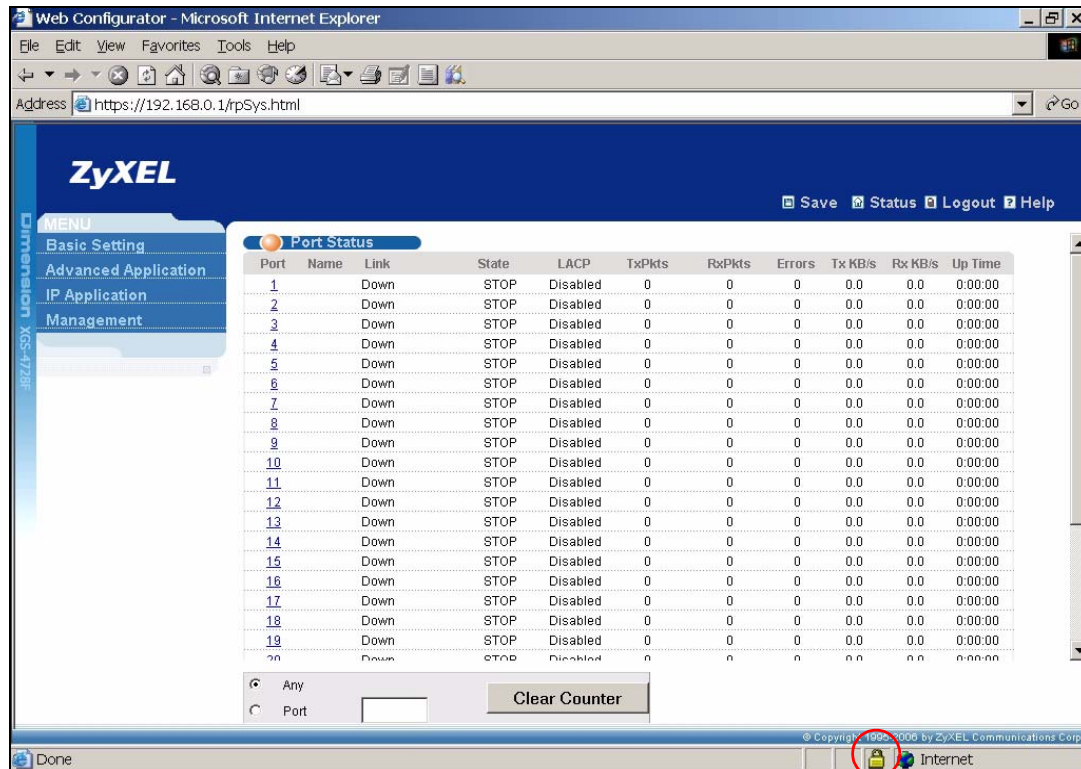
Figure 227 Security Certificate 2 (Netscape)



46.9.3 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 228 Example: Lock Denoting a Secure Connection



46.10 Service Port Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted

computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 229 Management > Access Control > Service Access Control

Services	Active	Service Port	Timeout
Telnet	☒	23	
SSH	☒	22	
FTP	☒	21	
HTTP	☒	80	3 Minutes
HTTPS	☒	443	
ICMP	☒		
SNMP	☒		

Apply Cancel

The following table describes the fields in this screen.

Table 155 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 Server Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click 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.

46.11 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 230 Management > Access Control > Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	☒	0.0.0.0	0.0.0.0	☒	☒	☒	☒	☒	☒	☒
2	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
3	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
4	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
5	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
6	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
7	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
8	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
9	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
10	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
11	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
12	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
13	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
14	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
15	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
16	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 156 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	Configure the IP address range of trusted computers from which you can manage this Switch.
End Address	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.

Table 156 Management > Access Control > Remote Management (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.

Diagnostic

This chapter explains the **Diagnostic** screen.

47.1 Diagnostic

Click **Management > Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

Figure 231 Management > Diagnostic

The screenshot shows the 'Diagnostic' screen with a title bar. Below the title bar is a multi-line text box containing the following text:

```
Resolving 192.168.1.23 ... 192.168.1.23
Reply from 192.168.1.23
Reply from 192.168.1.23
Reply from 192.168.1.23
Reply from 192.168.1.23
Ping Host Successful
```

Below the text box are three sections:

- System Log:** Includes 'Display' and 'Clear' buttons.
- IP Ping:** Includes an 'IP Address' input field and a 'Ping' button.
- Ethernet Port Test:** Includes a 'Port' input field with the value '1' and a 'Port Test' button.

The following table describes the labels in this screen.

Table 157 Management > Diagnostic

LABEL	DESCRIPTION
System Log	Click Display to display a log of events in the multi-line text box. Click Clear to empty the text box and reset the syslog entry.

Table 157 Management > Diagnostic (continued)

LABEL	DESCRIPTION
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click Ping to have the Switch ping the IP address (in the field to the left).
Ethernet Port Test	Enter a port number and click Port Test to perform an internal loopback test.

This chapter explains the syslog screens.

48.1 Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 158 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.

48.2 Syslog Setup

Click **Management** > **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Figure 232 Management > Syslog

Logging type	Active	Facility
System	☒	local use 0
Interface	☒	local use 0
Switch	☒	local use 0
AAA	☒	local use 0
IP	☒	local use 0

The following table describes the labels in this screen.

Table 159 Management > Syslog

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.

48.3 Syslog Server Setup

Click **Management > Syslog > Syslog Server Setup** to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 233 Management > Syslog > Server Setup

The following table describes the labels in this screen.

Table 160 Management > Syslog > Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays Yes if the device is to send logs to the syslog server. No displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's Delete check box and click Delete to remove the entry.
Cancel	Click Cancel to begin configuring this screen afresh.

48.4 Syslog Messages

The following table shows log messages the Switch may generate.

Table 161 Syslog Messages

LOG TYPE	SEVERITY	MESSAGE
SP_SYSLOG_TYPE_AAA	SYSLOG_ERR	Authentication failure
SP_SYSLOG_TYPE_AAA	SYSLOG_INFO	SSH: User <username> login
SP_SYSLOG_TYPE_AAA	SYSLOG_INFO	SSH forced out by disabling multi-login
SP_SYSLOG_TYPE_AAA	SYSLOG_INFO	SSH forced out by local user
SP_SYSLOG_TYPE_AAA	SYSLOG_INFO	Telnet forced out by disabling multi-login
SP_SYSLOG_TYPE_AAA	SYSLOG_INFO	Telnet forced out by local user
SP_SYSLOG_TYPE_AAA	SYSLOG_INFO	User <username> login
SP_SYSLOG_TYPE_AAA	SYSLOG_INFO	User <username> logout
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	CLI user <username> login
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	FTP authentication failure [username: <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	Console authentication failure [username: <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	HTTP(s) authentication failure [username: <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	HTTP(s) authorization failure [username: <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	SSH authentication failure [username: <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	Telnet authentication failure [username: <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	Telnet authorization failure [username: <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	802.1x Authentication failure [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_NOTICE	802.1x Authorization failure [User-Name <username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x Authentication - retransmit EAPOL-START packet [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x RADIUS server timeout [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Invalid Tunnel-Type <type> [User-Name <username>] [NAS-Port <port>]

Table 161 Syslog Messages

LOG TYPE	SEVERITY	MESSAGE
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Invalid Tunnel-Medium-Type <type> [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Less or more VLAN attributes [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Too many bandwidth attributes [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Invalid bandwidth format <Ingress Egress> [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Invalid VLAN-ID <VLAN ID> [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Invalid VLAN setting, the switch is with port-based VLAN
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Static VLAN <VLAN ID> does not exist [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Ingress bandwidth <bandwidth> is out of range [User-name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Egress bandwidth <bandwidth> is out of range [User-name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	802.1x - Bandwidth conflicts with current link aggregation settings [User-Name <username>] [NAS-Port <port>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	RADIUS Accounting - change RADIUS accounting server from <index> to <index>
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	RADIUS Accounting server <index> becomes reachable
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	RADIUS Accounting server <index> is unreachable
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	RADIUS Authentication - change RADIUS server from <index> to <index>
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	RADIUS server <index> is unreachable
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	RADIUS server <index> becomes reachable
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	Invalid Service Type: USER [<username>]

Table 161 Syslog Messages

LOG TYPE	SEVERITY	MESSAGE
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	Privilege out of range: USER [<username>]
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	TACAS+ account server <index> becomes reachable
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	TACAS+ account server <index> is unreachable
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	TACAS+ server <index> becomes reachable
SP_SYSLOG_TYPE_AAA	SYSLOG_WARNING	TACAS+ server <index> is unreachable
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_DEBU	Port <port> link up
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_DEBU	Port <port> link down
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_INFO	LLDP Remote topologyChange
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Temperature Over Alarm High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Temperature Over Warn High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Temperature Under Alarm Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Temperature Under Warn Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Voltage Over Alarm High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Voltage Over Warn High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Voltage Under Alarm Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Voltage Under Warn Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Bias Over Alarm High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTE RFACE	SYSLOG_NOTICE	Bias Over Warn High Threshold(<threshold>) On Port <port>, Current Value : <value>

Table 161 Syslog Messages

LOG TYPE	SEVERITY	MESSAGE
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	Bias Under Alarm Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	Bias Under Warn Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	TxPower Over Alarm High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	TxPower Over Warn High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	TxPower Under Alarm Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	TxPower Under Warn Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	RxPower Over Alarm High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	RxPower Over Warn High Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	RxPower Under Alarm Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	RxPower Under Warn Low Threshold(<threshold>) On Port <port>, Current Value : <value>
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	Abnormal temperature state at port <port> has been cleared
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	Abnormal voltage state at port <port> has been cleared
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	Abnormal TX bias state at port <port> has been cleared
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	Abnormal TX power state at port <port> has been cleared
SP_SYSLOG_TYPE_INTERRUPT	SYSLOG_NOTICE	Abnormal RX power state at port <port> has been cleared
SP_SYSLOG_TYPE_SWITCH	SYSLOG_ALERT	System has reset without management command
SP_SYSLOG_TYPE_SWITCH	SYSLOG_ALERT	Another image was booted
SP_SYSLOG_TYPE_SWITCH	SYSLOG_CRITICAL	<1.2VIN 1.8VIN 3.3VIN 2.5VIN> voltage value <value> is lower than its limit voltage value

Table 161 Syslog Messages

LOG TYPE	SEVERITY	MESSAGE
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_CRITICAL	system voltage has recovered to normal state
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_CRITICAL	<FAN1 FAN2> RPM value <value> is lower than its limit RPM value
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_CRITICAL	The RPM of the fan has recovered to normal state
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_EMERGEMC Y	<BOARD MAC PHY> temperature value <value> exceeds its limit temperature value
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_EMERGEMC Y	system temperature has recovered to normal state
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_ERR	Restore system configuration failed
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_ERR	Load factory default configuration failed
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_ERR	Gets the time and date from a time server failed
SP_SYSLOG_TYPE_IP	SYSLOG_INFO	Ping probe to <target ip address> failed
SP_SYSLOG_TYPE_IP	SYSLOG_INFO	Ping test to <target ip address> failed
SP_SYSLOG_TYPE_IP	SYSLOG_INFO	Ping test to <target ip address> completed
SP_SYSLOG_TYPE_IP	SYSLOG_INFO	Trace path to <target ip address> completed
SP_SYSLOG_TYPE_IP	SYSLOG_INFO	Trace path to <target ip address> failed
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Traffic of type <type> from port <port> is abnormal
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	System bootup
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	System init completed
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Save system configuration successfully
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Save system configuration <index> successfully
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Save system configuration failed
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Upgrade system firmware successfully
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Upgrade system firmware failed
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Restore system configuration successfully

Table 161 Syslog Messages

LOG TYPE	SEVERITY	MESSAGE
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_INFO	Load factory default configuration successfully
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	Gets the time and date from a time server successfully
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	PethPse Port OnOff Trap
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	PethPse Main Power Usage On Trap
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	PethPse Main Power Usage Off Trap
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	System cold start
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	System warm start
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	System has reset due to a management command
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	Port <port> loopguard
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	External alarm input(<index>)
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	External alarm input(<index>) clear
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	System reboot
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	MSTP instance <instance ID> new root
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	MSTP instance <instance ID> topology changes
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	Switch becomes MRSTP tree <index> new root
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	MRSTP tree <index> topology changes
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	Switch becomes the STP new root
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_NOTICE	STP topology changes
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	mac <MAC address> vlan <VLAN ID> ip <IP address> port <port> count <count> last update time <timestamp>
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	MAC address table is full
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	MAC address table is recovered to normal state
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	Hardware host table is full

Table 161 Syslog Messages

LOG TYPE	SEVERITY	MESSAGE
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	Port <port> link speed and duplex mode autonegotiation has failed
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	Port <port> link speed and duplex mode autonegotiation has recovered to normal state
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	CFM MEP ID <identifier> with MA Index <index> and MD Index <index> has no defects
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	CFM MEP ID <index> with MA Index <index> and MD Index <index> has <XconCCM defect ErrorCCM defect RemoteCCM defect MACstatus defect RDICCM defect>
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	RMON falling alarm
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	PoE overload event (port <port>)
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	PoE short-circuit event (port <port>)
SP_SYSLOG_TYPE_SWIT CH	SYSLOG_WARNING	PoE over system budget event (port <port>)

Cluster Management

This chapter introduces cluster management.

49.1 Clustering Management Status Overview

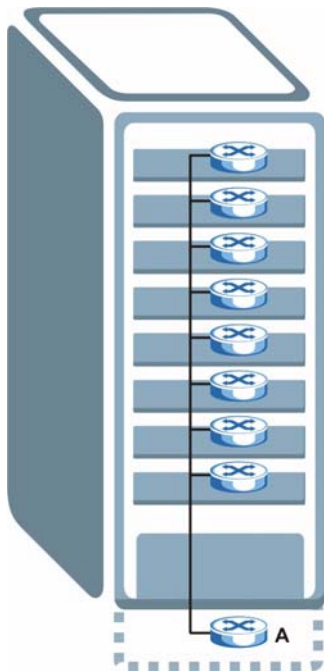
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 162 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Cluster member models must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The cluster manager is the Switch through which you manage the cluster member switches.
Cluster Members	Cluster members are the switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 234 Clustering Application Example



49.2 Cluster Management Status

Click **Management > Cluster Management** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 235 Management > Cluster Management

Clustering Management Status

Configuration

Status

Manager

Manager

00:13:49:01:1f:b0

The Number Of Member = 1

Index	MacAddr	Name	Model	Status
1	00:13:49:ae:fb:7a	ES-2024PWR	ES-2024PWR	Online

The following table describes the labels in this screen.

Table 163 Management > Cluster Management

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. Manager Member (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) None (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the Index column is a hyperlink leading to the cluster member switch's web configurator (see Figure 236 on page 438).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This field displays the model name.
Status	This field displays: Online (the cluster member switch is accessible) Error (for example, the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) Offline (the switch is disconnected - Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down)

49.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web

configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 236 Cluster Management: Cluster Member Web Configurator Screen



49.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 237 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 370lt0.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 164 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.
370lt0.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.

49.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 238 Management > Clustering Management > Configuration

Clustering Manager:

Active ☒

Name

VID

Clustering Candidate:

List

00:13:49:00:00:01/ES-2108-G/ES-2108-G
00:13:49:00:00:02/GS-3012/GS-3012

Password

Index	MacAddr	Name	Model	Remove
1	00:13:49:ae:fb:7a	ES-2024PWR	ES-2024PWR	☐

The following table describes the labels in this screen.

Table 165 Management > Clustering Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select Active to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen 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.

Table 165 Management > Clustering Management > Configuration (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.
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 and a warning icon () appears in the member summary list below. 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.
Remove	Select this checkbox and then click the Remove button to remove a cluster member switch from the cluster.
Cancel	Click Cancel to begin configuring this screen afresh.

MAC Table

This chapter introduces the **MAC Table** screen.

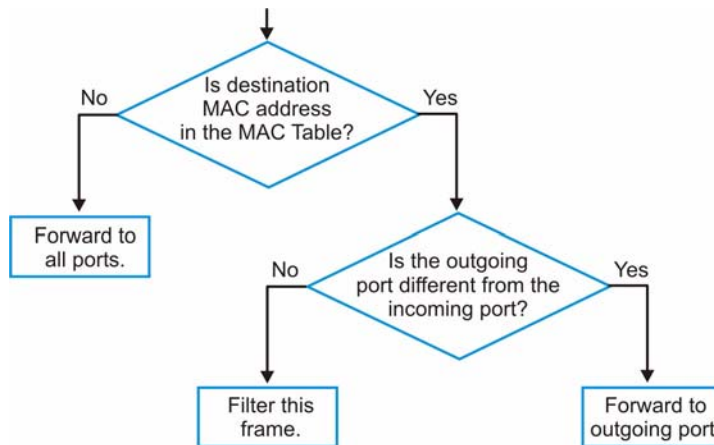
50.1 MAC Table Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's **MAC Table**. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

- 1 The Switch examines a received frame and learns the port from which this source MAC address came.
- 2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the **MAC Table**.
 - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.

- 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 239 MAC Table Flowchart

50.2 Viewing the MAC Table

Click **Management > MAC Table** in the navigation panel to display the following screen. Use this screen to search specific MAC addresses. You can also directly add dynamic MAC address(es) into the static MAC forwarding table or MAC filtering table from the MAC table using this screen.

Figure 240 Management > MAC Table

The interface shows the "MAC table" configuration page. It includes search and transfer options. The "Condition" section has radio buttons for "All", "Static", "MAC", "VID", and "Port". The "Sort by" dropdown is set to "MAC". The "Transfer Type" section has radio buttons for "Dynamic to MAC forwarding" and "Dynamic to MAC filtering". Below these are "Search", "Transfer", and "Cancel" buttons.

Index	MAC Address	VID	Port	Type
1	00:02:e3:57:ea:1c	1	1	dynamic
2	00:04:11:9b:78:00	1	1	dynamic
3	00:11:00:f5:12:92	1	CPU	static
4	00:0e:00:11:60:10	1	1	dynamic
5	00:0f:fe:1e:00:11	1	1	dynamic

The following table describes the labels in this screen.

Table 166 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select All to display all MAC addresses in the MAC table. Select Static to only display static MAC address(es) in this screen. Select MAC and enter a valid MAC address (six hexadecimal character pairs) to display the MAC address information in this screen. Select VID and type a VLAN identification number to display all MAC addresses in the VLAN. Select Port and type the number of a port to display all MAC addresses learned from the port.
Sort by	Select this to display and arrange the data according to MAC address (MAC), VLAN group (VID) or port number (Port). The information is then displayed in the summary table below.
Transfer Type	Select Dynamic to MAC forwarding and click Transfer to add the relative dynamic MAC address(es) you select the criteria here into the static MAC forwarding table (see Section 10.2 on page 137). The type of the MAC address(es) will be changed to "static". Select Dynamic to MAC filtering and click Transfer to add the relative dynamic MAC address(es) you make the search here into the static MAC filtering table (see Section 12.1 on page 145). The MAC address(es) will be removed from the MAC table and all traffic sent from the MAC address(es) will be blocked by the Switch.
Search	Click this to search data in the MAC table according to your input criteria.
Transfer	Click this to perform the MAC address transferring you selected in the Transfer Type field.
Cancel	Click this to begin configuring the search criteria afresh.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the Static MAC Forwarding screen).

IP Table

This chapter introduces the IP table.

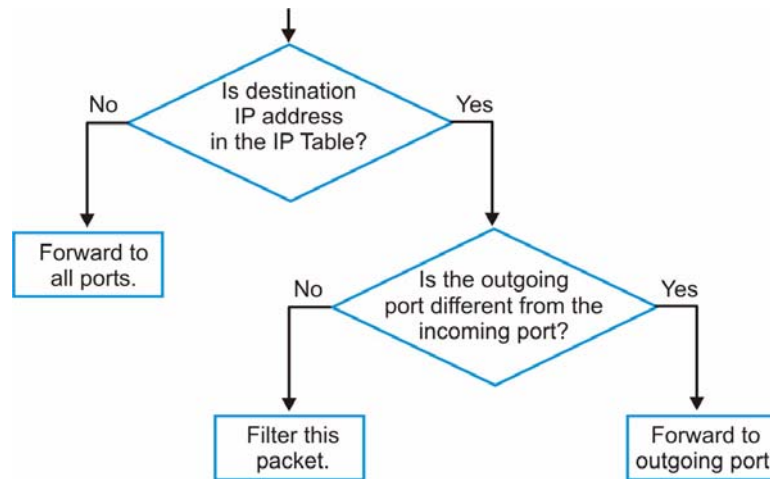
51.1 IP Table Overview

The **IP Table** screen shows how packets are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the IP address of the device is shown on the Switch's **IP Table**. The **IP Table** also shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

The Switch uses the **IP Table** to determine how to forward packets. See the following figure.

- 1 The Switch examines a received packet and learns the port from which this source IP address came.
- 2 The Switch checks to see if the packet's destination IP address matches a source IP address already learned in the **IP Table**.
 - If the Switch has already learned the port for this IP address, then it forwards the packet to that port.
 - If the Switch has not already learned the port for this IP address, then the packet is flooded to all ports. Too much port flooding leads to network congestion.

- If the Switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

Figure 241 IP Table Flowchart

51.2 Viewing the IP Table

Click **Management > IP Table** in the navigation panel to display the following screen.

Figure 242 Management > IP Table

IP Table				
Sort by IP VID Port				
Index	IP Address	VID	Port	Type
1	192.168.1.5	1	6	dynamic
2	192.168.1.10	0	CPU	static
3	192.168.1.255	0	CPU	static

The following table describes the labels in this screen.

Table 167 Management > IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.

Table 167 Management > IP Table (continued)

LABEL	DESCRIPTION
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays CPU to indicate the IP address belongs to the Switch.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

ARP Table

This chapter introduces ARP Table.

52.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

52.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

52.2 The ARP Table Screen

Click **Management > ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s) and remove specific dynamic ARP entries.

Figure 243 Management > ARP Table

Index	IP Address	MAC Address	VID	Port	Type
1	10.1.2.2	00:19:cb:6f:91:59	1	0	static
2	192.168.1.2	00:19:cb:6f:91:59	1	0	static
3	192.168.1.103	00:21:85:0c:44:4b	1	8	dynamic
4	192.168.10.2	00:19:cb:6f:91:59	102	0	static

The following table describes the labels in this screen.

Table 168 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 learned 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 learned IP address is the Switch's management IP address.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the Static MAC Forwarding screen).

Routing Table

This chapter introduces the routing table.

53.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach. The Switch automatically updates the routing table with the RIP information received from other Ethernet devices.

53.2 Viewing the Routing Table Status

Use this screen to view routing table information. Click **Management > Routing Table** in the navigation panel to display the screen as shown.

Figure 244 Management > Routing Table

Routing Table Status					
Index	Destination	Gateway	Interface	Metric	Type
1	192.168.1.0/24	192.168.1.1	192.168.1.1	1	STATIC
2	10.10.10.0/24	10.10.10.1	10.10.10.1	1	STATIC

The following table describes the labels in this screen.

Table 169 Management > Routing Table

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route; OSPF - added as an OSPF interface, RIP - learned from incoming RIP packets or STATIC - added as a static entry.

Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

54.1 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management > Configure Clone** to open the following screen.

Figure 245 Management > Configure Clone

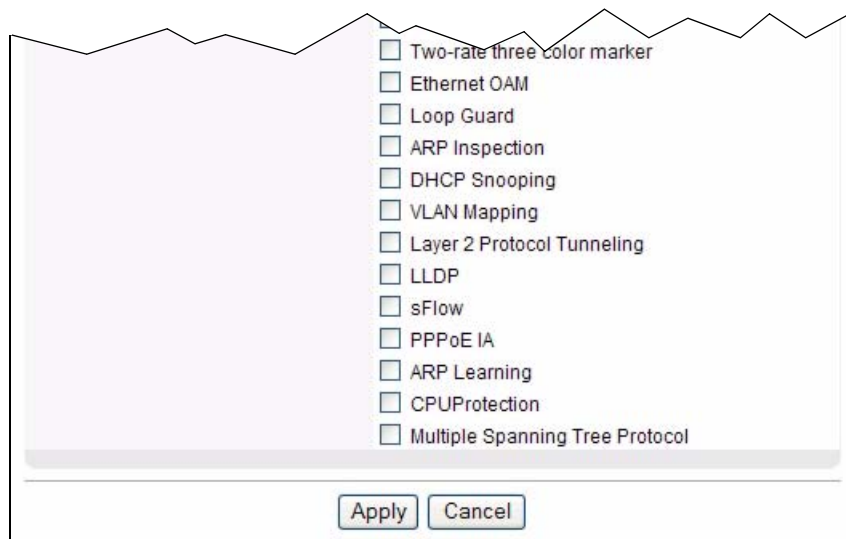
Configure Clone

Source Port Destination

Port Features

Basic Setting

- ☐ Active
- ☐ Name
- ☐ Speed / Duplex
- ☐ BPDU Control
- ☐ Flow Control
- ☐ Intrusion Lock
- ☐ VLAN1q
- ☐ VLAN1q Member
- ☐ Bandwidth Control
- ☐ VLAN Stacking
- ☐ Port Security
- ☐ Broadcast Storm Control
- ☐ Mirroring
- ☐ Port Authentication
- ☐ Queuing Method
- ☐ IGMP Filtering
- ☐ Spanning Tree Protocol



The following table describes the labels in this screen.

Table 170 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.
Basic Setting	Select which port settings (configured in the Basic Setting menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (configured in the Advanced Application menus) should be copied to the destination ports.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

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](#)

55.1 Power, Hardware Connections, and LEDs

The Switch does not turn on. None of the LEDs turn on.

- 1 Make sure the Switch is turned on (in DC models or if the DC power supply is connected in AC/DC models).
- 2 Make sure you are using the power adaptor or cord included with the Switch.
- 3 Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
- 5 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
- 6 If the problem continues, contact the vendor.

The **ALM** LED is on.

- 1 Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
- 2 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
- 3 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 3.3 on page 45](#).
- 2 Check the hardware connections. See [Section 3.1 on page 37](#).
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
- 5 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
- 6 If the problem continues, contact the vendor.

55.2 Switch Access and Login

I forgot the IP address for the Switch.

- 1 The default in-band IP address is **192.168.1.1**.
- 2 Use the console port to log in to the Switch.
- 3 Use the **MGMT** port to log in to the Switch, the default IP address of the **MGMT** port is 192.168.0.1.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 4.6 on page 54](#).

I forgot the username and/or password.

- 1 The default username is **admin** and the default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 4.6 on page 54](#).

I cannot see or access the **Login** screen in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default in-band IP address is **192.168.1.1**.
 - If you changed the IP address, use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Switch](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 3.3 on page 45](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)
- 5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See [Section 4.6 on page 54](#).
- 6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Switch.

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
- 3 Disconnect and re-connect the cord to the Switch.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 4.6 on page 54](#).

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

I cannot see some of **Advanced Application** submenus at the bottom of the navigation panel.

The recommended screen resolution is 1024 by 768 pixels. Adjust the value in your computer and then you should see the rest of **Advanced Application** submenus at the bottom of the navigation panel.

There is unauthorized access to my Switch via telnet, HTTP and SSH.

Click the **Display** button in the **System Log** field in the **Management** > **Diagnostic** screen to check for unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **Management** > **Access Control** > **Remote Management** screen for telnet, HTTP and SSH (see [Section 46.11 on page 420](#)). Computers not belonging to the secured client set cannot get permission to access the Switch.

55.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's nonvolatile memory each time you make changes. Click **Save** at the top right corner of the web configurator to save the configuration permanently. See also [Section 45.3 on page 390](#) for more information about how to save your configuration.



Product Specifications

The following tables summarize the Switch's hardware and firmware features.

Table 171 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	Standard 19" rack mountable 438 mm (W) x 310 mm (D) x 44.45 mm (H)
Weight	XGS-4526: 4.75 Kg XGS-4528F or XGS-4728F: 4.9 Kg
Power Specification	XGS-4526: AC: 100 - 240 VAC 50/60 Hz 0.8 A max, 72 W internal universal power supply XGS-4528F or XGS-4728F: AC: 100 - 240 VAC 50/60 Hz 0.8 A max, 85 W internal universal power supply DC: -36 VDC ~ -72 VDC 2.3 A max, 80 W consumption. There is no tolerance for the DC input voltage. One Backup Power Supply (BPS) connector
Interfaces	XGS-4526: 20 Gigabit Ethernet (GbE) copper ports plus 4 Dual Personality interfaces. XGS-4528F or XGS-4728F: 24 Gigabit Ethernet (GbE) Dual Personality interfaces. Each Dual Personality interface has: • a 1000Base-T port, compatible with Cat5/5e/6 copper cable. • a mini-GBIC slot, compatible with Small Form-Factor Pluggable (SFP) Multi Source Agreement (MSA) transceivers, to be used with 1000Base-X fiber cables. For each Dual Personality interface one port or slot is active at a time. Two stacking ports (XGS-4528F and XGS-4728F only) One optional uplink module set. One local management Ethernet 10/100Base-T port One RS-232 console port

Table 171 Hardware Specifications

Ethernet Ports	Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. 1000 Mbps and 10 Gbps in full duplex. Auto-crossover: Use either crossover or straight-through Ethernet cables. Auto-MDIX Compliant with IEEE 802.3ad/u/x Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x)
LEDs	Main switch: BPS, PWR, SYS, ALM, Per Stacking port: S1, S2 (XGS-4528F and XGS-4728F only) Per mini-GBIC port: green LED Per 1000Base-T port: Green: 10/1000 Mbps Amber: 100 Mbps mini-GBIC/1000Base-T LEDs: steady: link state blinking: transmitting/receiving
Operating Environment	Temperature: 0° C ~ 45° C (32° F ~ 113° F) Humidity: 10 ~ 90% (non-condensing)
Storage Environment	Temperature: -10° C ~ 70° C (-13° F ~ 158° F) Humidity: 10 ~ 90% (non-condensing)
Ground Wire Gauge	18 AWG or larger
Power Wire Gauge	18 AWG or larger
Fuse Specification	250 VAC, T4A. For DC version switchboard.
Approvals	Safety UL 60950-1, CSA 60950-1, EN 60950-1, IEC 60950-1 EMC FCC Part 15 (Class A), CE EMC (Class A)

Table 172 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	In band: 192.168.1.1 Out of band (Management port): 192.168.0.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234

Table 172 Firmware Specifications

FEATURE	DESCRIPTION
Number of Login Accounts Configurable on the Switch	4 management accounts configured on the Switch. Authentication via RADIUS and TACACS+ also available.
IP Routing Domain	An IP interface (also known as an IP routing domain) is not bound to a physical port. Configure an IP routing domain to allow the Switch to route traffic between different networks.
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
VLAN Stacking	Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the Switch assign IP addresses, an IP default gateway and DNS servers to computers on your network.
IGMP Snooping	The Switch supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your Switch.
Differentiated Services (DiffServ)	With DiffServ, the Switch marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Classifier and Policy	You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc.
Queuing	Queuing is used to help solve performance degradation when there is network congestion. Three scheduling services are supported: Strict Priority Queuing (SPQ), Weighted Round Robin (WRR) and Weighted Fair Queuing (WFQ). This allows the Switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Table 172 Firmware Specifications

FEATURE	DESCRIPTION
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
IP Multicast	With IP multicast, the Switch delivers IP packets to a group of hosts on the network - not everybody. In addition, the Switch can send packets to Ethernet devices that are not VLAN-aware by untagging (removing the VLAN tags) IP multicast packets.
RIP	RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers.
OSPF	OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information. OSPF is best suited for large networks.
DVMRP	DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol.
VRRP	Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)/MSTP (Multiple Spanning Tree Protocol)	(M)(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (M)(R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.
Loop Guard	Use the loop guard feature to protect against network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized DHCP and ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.
Authentication, Authorization and Accounting	The Switch supports authentication, authorization and accounting services via RADIUS and TACACS+ AAA servers.

Table 172 Firmware Specifications

FEATURE	DESCRIPTION
Device Management	Use the web configurator or commands to easily configure the rich range of features on the Switch.
Port Cloning	Use the port cloning feature to copy the settings you configure on one port to another port or ports.
Syslog	The Switch can generate syslog messages and send it to a syslog server.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or an FTP/TFTP tool to put it on the Switch. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.
Cluster Management	Cluster management (also known as iStacking) 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.
sFlow	sFlow allows the Switch to monitor traffic in a network by getting sample data and packet statistics from traffic, and send information to an sFlow collector for analysis.
PPPoE IA	With the PPPoE Intermediate Agent enabled, the Switch can give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.
CPU Protection	You can limit the rate of protocol control packets (such as ARP, BPDU and/or IGMP) to be delivered to the CPU on a port.
Error Disable	You can 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. You can also configure the Switch to automatically undo the action after the error is gone.
Private VLAN	You can set the Switch to prevent communications between ports in a VLAN to do port isolation within a VLAN.
Policy Routing	Policy routing lets you override the default routing behavior and alter the packet forwarding based on the pre-defined policy.
ARP Learning	You can configure the Switch to update the ARP table with with an ARP reply or a gratuitous ARP request and/or an APR request.
Load Sharing	Load sharing allows the Switch to forward packets destined to the same device through different routing paths of equal path cost.

Table 173 Switching Specifications

Layer 2 Features	Bridging	8K MAC addresses in the XGS-4526 or XGS-4528F; 16K MAC addresses in the XGS-4728F Static MAC address filtering by source/destination Broadcast storm control Static MAC address forwarding
	Switching	Switching fabric: 144 Gbps, non-blocking Maximum frame size: 9 k bytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets
	STP	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Multiple Rapid Spanning Tree capability (4 configurable trees) IEEE 802.1s Multiple Spanning Tree Protocol BPDU transparency Smart isolation
	QoS	IEEE 802.1p Eight priority queues per port Port-based egress traffic shaping Rule-based traffic mirroring IEEE 802.3x flow control TRTCM
	VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K, 1K static maximum Supports GVRP Double tagging for VLAN stacking Protocol Based VLAN Subnet Based VLAN Selective Q-in-Q VLAN translation (mapping) Private VLAN
	Port Aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking 12 groups (up to 8 ports each)

Table 173 Switching Specifications (continued)

	Port mirroring	All ports support port mirroring Supports port mirroring per IP/TCP/UDP
	Bandwidth control	Supports rate limiting at 64K increment Supports CIR/PIR for ingress bandwidth control
Layer 3 Features	IP Capability	IPv4 support 128 IP routing domains 2K IP address table in the XGS-4526 or XGS-4528F; 8K IP address table in the XGS-4728F 512 routing paths in the XGS-4526 or XGS-4528F; 8K routing paths in the XGS-4728F Wire speed IP forwarding
	IPv6	MLD snooping proxy (XGS-4728F only) DHCPv6: client and relay ICMPv6 IPv6 Path MTU NDP: host and router IPv6 address stateless auto-configuration: host and router IPv6 static route
	Routing protocols	Unicast: RIP-V1/V2, OSPF V2 Multicast: DVMRP, IGMP V1/V2/V3 Static Routing
	IP services	DHCP relay; VLAN based DHCP server/relay Policy routing Load sharing 64 VRRP entries
Filtering	Support L2 MAC filtering, L3 IP filtering, Layer 4 TCP/UDP socket	
Multicast	IGMP snooping (IGMP v1/v2/v3, 16 VLAN maximum-user configurable) IGMP filtering 5 MVR entries IGMP timer Multicast reserve group Static multicast IGMP snooping fast-leave IGMP snooping statistics IGMP throttling	

Table 173 Switching Specifications (continued)

AAA	Support RADIUS and TACACS+
Security	IEEE 802.1x port-based authentication Static MAC address filtering Static MAC address forwarding MAC Freeze Limiting number of dynamic addresses per port Intrusion lock IP source guard Static IP/MAC binding DHCP snooping ARP inspection MAC authentication Guest VLAN PPPoE IA and option 82 Configurable ARP learning mode
Management	IEEE 802.3ah OAM IEEE 802.1AB LLDP IEEE 802.1ag CFM Loop guard Password encryption sFlow User access right Error disable

The following list, which is not exhaustive, illustrates the standards supported in the Switch.

Table 174 Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 894	Ethernet II Encapsulation
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1155	SMI
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II

Table 174 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2131, RFC 2132	Dynamic Host Configuration Protocol (DHCP)
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2139	RADIUS Accounting
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2338	Virtual Router Redundancy Protocol (VRRP)
RFC 2698	Two Rate Three Color Marker (TRTCM)
RFC 2865	RADIUS - Vendor Specific Attribute
RFC 2674	P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 3046	DHCP Relay
RFC 3164	Syslog
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3)
RFC 3580	RADIUS - Tunnel Protocol Attribute
IEEE 802.1AB	Link Layer Discovery Protocol (LLDP)
IEEE 802.1ag	Connectivity Fault Management (CFM)
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1D	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1Q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation
IEEE 802.3ah	Ethernet OAM (Operations, Administration and Maintenance)
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BASE-X For optical fiber link 1000BASE-SX/LX.
RFC 2516	A method for transmitting PPP over Ethernet (PPPoE)
RFC 3176	sFlow
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

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 175 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.

Table 175 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.

Table 175 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
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).

Table 175 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

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

CE Mark Warning:

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

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

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

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

Numerics

802.1P priority [114](#)

A

access control

limitations [397](#)

login account [412](#)

remote management [420](#)

service port [419](#)

SNMP [398](#)

accounting

setup [249](#)

address learning, MAC [127](#), [129](#)

Address Resolution Protocol (ARP) [381](#), [451](#), [455](#), [456](#)

administrator password [412](#)

age [163](#)

aggregator ID [181](#), [183](#)

aging time [109](#)

applications

bridging [27](#)

IEEE 802.1Q VLAN [29](#)

switched workgroup [28](#)

Area Border Router (ABR) [332](#)

area ID

and OSPF [338](#)

ARP

how it works [381](#), [451](#)

table [452](#)

ARP (Address Resolution Protocol) [381](#), [451](#)

ARP inspection [259](#), [262](#)

and MAC filter [262](#)

configuring [263](#)

syslog messages [263](#)

trusted ports [263](#)

AS Boundary Router [332](#)

authentication [338](#)

and OSPF [337](#)

and RADIUS [244](#)

setup [249](#)

authorization

privilege levels [251](#)

setup [249](#)

automatic VLAN registration [118](#)

Autonomous System

and OSPF [331](#)

Autonomous System (AS) [331](#), [349](#)

B

back up, configuration file [393](#)

Backbone Router (BR) [332](#)

backbone, routing [331](#)

Backup Designated Router(BDR), and OSPF [333](#)

bandwidth control [468](#)

basic settings [101](#)

basic setup tutorial [63](#)

BDR (Backup Designated Router) [333](#)

binding [259](#)

binding table [259](#)

building [259](#)

BPDUs (Bridge Protocol Data Units) [148](#)

Bridge Protocol Data Units (BPDUs) [148](#)

bridging [468](#)

C

CDP [294](#)

certifications [477](#)

notices [478](#)

viewing [479](#)

CFI (Canonical Format Indicator) [117](#)

changing the password [53](#)

Cisco Discovery Protocol, see CDP

CIST [152](#)

CIST (Common and Internal Spanning Tree)
[150](#)

Class of Service (CoS) [353](#)

classifier [201](#), [203](#)

and QoS [201](#)

editing [204](#)

example [206](#)

overview [201](#)

setup [201](#), [203](#), [204](#)

viewing [204](#)

cloning a port See port cloning

cluster management [435](#)

and switch passwords [441](#)

cluster manager [435](#), [440](#)

cluster member [435](#), [441](#)

cluster member firmware upgrade [439](#)

network example [436](#)

setup [440](#)

specification [435](#)

status [436](#)

switch models [435](#)

VID [440](#)

web configurator [437](#)

cluster manager [435](#)

cluster member [435](#)

command interface [31](#)

Common and Internal Spanning Tree (CIST)
[150](#)

Common and Internal Spanning Tree, See CIST
[152](#)

configuration [321](#)

change running config [391](#)

configuration file [55](#)

backup [393](#)

restore [55](#), [392](#)

saving [390](#)

configuration, saving [54](#)

console port

settings [44](#)

copying port settings, See port cloning

copyright [477](#)

CPU management port [132](#)

CPU protection

configuration [310](#)

overview [309](#)

current date [105](#)

current time [105](#)

D

Database Description (DD) [332](#)

daylight saving time [105](#)

default gateway [368](#)

Designated Router(DR), and OSPF [333](#)

DHCP [361](#)

client IP pool [368](#)

configuration options [361](#)

modes [361](#)

relay agent [361](#)

relay example [369](#)

server [361](#)

setup [367](#)

DHCP (Dynamic Host Configuration Protocol)
[361](#)

DHCP relay option 82 [261](#)

DHCP snooping [63](#), [259](#), [260](#)

configuring [261](#)

DHCP relay option 82 [261](#)

trusted ports [260](#)

untrusted ports [260](#)

DHCP snooping database [260](#)

diagnostics [423](#)

Ethernet port test [424](#)

ping [424](#)

system log [423](#)

Differentiated Service (DiffServ) [353](#)

DiffServ [353](#)

activate [356](#)

and TRTCM [358](#)

DS field [353](#)

DSCP [353](#)

DSCP-to-IEEE802.1p mapping [359](#)

network example [354](#)

PHB [353](#)

dimensions [463](#)

disclaimer [477](#)

double-tagged frames [219](#)

DR (Designated Router) [333](#)

DS (Differentiated Services) [353](#)

DSCP

DSCP-to-IEEE802.1p mapping [359](#)

service level [353](#)

what it does [353](#)

DSCP (DiffServ Code Point) [353](#)

DVMRP

- Autonomous System [349](#)
- default timer setting [352](#)
- error message [351](#)
- graft [350](#)
- how it works [349](#)
- implementation [349](#)
- probe [350](#)
- prune [350](#)
- report [350](#)
- setup [350](#)
- terminology [350](#)
- threshold [351](#)
- DVMRP (Distance Vector Multicast Routing Protocol) [349](#)
- dynamic link aggregation [177](#)

E

- egress port [135](#)
- Error Disable [77](#)
- error disable detect [311](#)
- error disable recovery
 - configuration [313](#)
 - overview [309](#)
- Ethernet broadcast address [381](#), [451](#)
- Ethernet port test [424](#)
- Ethernet ports [38](#)
 - default settings [39](#)
- example
 - summary address [341](#)
- exchange RIP and OSPF information [339](#)
- external authentication server [244](#)

F

- fan speed [103](#)
- FCC interference statement [477](#)
- file transfer using FTP
 - command example [394](#)
- filename convention, configuration
 - configuration
 - file names [393](#)
- filtering [145](#)
 - rules [145](#)

- filtering database, MAC table [443](#)
- firmware [102](#)
 - upgrade [391](#), [439](#)
- flow control [114](#)
 - back pressure [114](#)
 - IEEE802.3x [114](#)
- forwarding
 - delay [163](#)
- frames
 - tagged [125](#)
 - untagged [125](#)
- front panel [37](#)
- FTP [31](#), [393](#)
 - file transfer procedure [394](#)
 - restrictions over WAN [395](#)

G

- GARP [118](#)
- GARP (Generic Attribute Registration Protocol) [118](#)
- GARP terminology [118](#)
- GARP timer [109](#), [118](#)
- general features [468](#)
- general setup [104](#)
- getting help [56](#)
- GMT (Greenwich Mean Time) [105](#)
- GVRP [118](#), [125](#)
 - and port assignment [125](#)
- GVRP (GARP VLAN Registration Protocol) [118](#)

H

- hardware installation [33](#)
 - mounting [34](#)
- hardware monitor [102](#)
- hardware overview [37](#)
- hello time [163](#)
- hops [163](#)
- HTTPS [415](#)
 - certificates [415](#)
 - implementation [415](#)
 - public keys, private keys [415](#)

HTTPS example [416](#)

humidity [464](#)

I

IEEE 802.1p, priority [109](#)

IEEE 802.1x

 activate [190, 194, 247](#)

 reauthentication [191](#)

IEEE 802.1x, port authentication [187](#)

IGMP [349](#)

 how it works [346](#)

 overview [345](#)

 port based [347](#)

 setup [348](#)

 version [227](#)

 version 3 [347](#)

 versions supported [346](#)

IGMP (Internet Group Management Protocol)
[227, 346](#)

IGMP filtering [227](#)

 profile [233](#)

 profiles [229](#)

IGMP leave timeout

 fast [231](#)

 normal [230](#)

IGMP snooping [228](#)

 MVR [235](#)

IGMP throttling [231](#)

ingress port [135](#)

Installation

 Rack-mounting [34](#)

installation

 freestanding [33](#)

 precautions [34](#)

interface [334](#)

 and OSPF [341](#)

interface, and OSPF [332](#)

Internal Router (IR) [332](#)

Internet Protocol version 6, see IPv6

introduction [27](#)

IP

 capability [469](#)

 interface [110, 373](#)

 routing domain [110](#)

 services [469](#)

 setup [110](#)

IP multicast example [345](#)

IP source guard [259](#)

 ARP inspection [259, 262](#)

 DHCP snooping [259, 260](#)

 static bindings [259](#)

IP table [447](#)

 how it works [447](#)

IPv6 [30](#)

 Neighbor Discovery Protocol [30](#)

 ping [30](#)

L

L2PT [291](#)

 access port [292](#)

 CDP [291](#)

 configuration [293](#)

 encapsulation [291](#)

 LACP [291](#)

 MAC address [291](#)

 mode [292](#)

 overview [291](#)

 PAGP [291](#)

 point to point [291](#)

 STP [291](#)

 tunnel port [292](#)

 UDLD [291](#)

 VTP [291](#)

LACP [177, 294](#)

 system priority [184](#)

 timeout [184](#)

layer 2 features [468](#)

Layer 2 protocol tunneling, see L2PT

layer 3 features [469](#)

LEDs [45](#)

limit MAC address learning [199](#)

Link Aggregate Control Protocol (LACP) [177](#)

link aggregation [177](#)

 dynamic [177](#)

 ID information [178](#)

 setup [181, 183](#)

 status [179](#)

 traffic distribution algorithm [180](#)

 traffic distribution type [182](#)

- link state database [332](#), [335](#)
- lockout [54](#)
- log [423](#)
- login [47](#)
 - password [53](#)
- login account
 - Administrator [412](#)
 - non-administrator [412](#)
- login accounts [412](#)
 - configuring via web configurator [412](#)
 - multiple [412](#)
 - number of [412](#)
- login password [413](#)
- loop guard [283](#)
 - how it works [284](#)
 - port shut down [285](#)
 - probe packet [284](#)
- loop guard, vs STP [283](#)
- LSA (Link State Advertisement) [332](#)

M

- MAC (Media Access Control) [102](#)
- MAC address [102](#), [381](#), [451](#)
 - maximum number per port [199](#), [200](#)
- MAC address learning [109](#), [127](#), [129](#), [137](#), [199](#)
 - specify limit [199](#)
- MAC authentication [188](#)
 - aging time [195](#)
- MAC filter
 - and ARP inspection [262](#)
- MAC freeze [198](#)
- MAC table [443](#)
 - how it works [443](#)
 - viewing [444](#)
- maintenance
 - configuration backup [393](#)
 - firmware [391](#)
 - restoring configuration [392](#)
- maintenance [389](#)
 - current configuration [389](#)
 - main screen [389](#)
- Management Information Base (MIB) [398](#)
- management port [135](#)
- managing the device

- good habits [31](#)
 - using FTP. See FTP.
 - using SNMP. See SNMP.
 - using Telnet. See command interface.
 - using the command interface. See command interface.
 - using the web configurator. See web configurator.
- man-in-the-middle attacks [262](#)
- max
 - age [163](#)
 - hops [163](#)
- metric [340](#)
- MIB
 - and SNMP [398](#)
 - supported MIBs [399](#)
- MIB (Management Information Base) [398](#)
- mini GBIC ports [39](#)
 - connection speed [39](#)
 - connector type [39](#)
 - transceiver installation [39](#)
 - transceiver removal [40](#)
- mirroring ports [175](#)
- monitor port [175](#), [176](#)
- mounting brackets [34](#)
- MSA (MultiSource Agreement) [39](#)
- MST Instance, See MSTI [151](#)
- MST region [151](#)
- MSTI [151](#)
 - MST ID [151](#)
- MSTI (Multiple Spanning Tree Instance) [150](#)
- MSTP [147](#), [150](#)
 - bridge ID [167](#)
 - configuration [162](#), [165](#)
 - configuration digest [167](#)
 - forwarding delay [163](#)
 - Hello Time [167](#)
 - hello time [163](#)
 - Max Age [167](#)
 - max age [163](#)
 - max hops [163](#)
 - MST region [151](#)
 - network example [150](#)
 - path cost [164](#)
 - port priority [164](#)
 - revision level [163](#)
- MSTP (Multiple Spanning Tree Protocol) [147](#)

MTU (Multi-Tenant Unit) [106](#)

multicast [227](#)

802.1 priority [229](#)

and IGMP [227](#)

IGMP throttling [231](#)

IP addresses [227](#)

overview [227](#)

setup [229](#)

multicast delivery tree [350](#)

multicast group [233](#)

multicast router ('mrouter') [350](#)

multicast VLAN [239](#)

Multiple Spanning Tree Instance, See MSTI [150](#)

Multiple Spanning Tree Protocol [149](#)

Multiple Spanning Tree Protocol, See MSTP. [147](#)

Multiple STP [149](#)

Multiple STP, see MSTP [150](#)

MVR [235](#)

configuration [237](#)

group configuration [239](#)

network example [235](#)

MVR (Multicast VLAN Registration) [235](#)

N

network management system (NMS) [398](#)

NTP (RFC-1305) [105](#)

O

OSPF [331](#)

advantages [331](#)

area [331](#), [337](#)

Area 0 [331](#)

area ID [338](#)

authentication [337](#), [338](#)

autonomous system [331](#)

backbone [331](#)

configuration steps [333](#)

general settings [336](#)

how it works [332](#)

interface [332](#), [334](#), [341](#)

link state database [332](#), [335](#)

network example [332](#)

priority [333](#)

redistribute route [340](#)

route cost [338](#)

router elections [333](#)

router ID [336](#)

router types [332](#)

status [334](#)

stub area [331](#), [338](#)

virtual link [333](#)

virtual links [343](#)

vs RIP [331](#)

OSPF (Open Shortest Path First) [331](#)

OSPF redistribution [339](#)

P

PAGP [294](#)

password [53](#)

administrator [412](#)

PHB (Per-Hop Behavior) [353](#)

ping, test connection [424](#)

policy [209](#), [212](#), [326](#)

and classifier [209](#), [326](#)

and DiffServ [207](#)

configuration [209](#), [326](#)

example [213](#)

overview [207](#)

rules [207](#), [208](#)

viewing [211](#)

policy configuration [212](#)

policy routing

benefits [323](#)

cost savings [323](#)

load sharing [323](#)

overview [323](#)

policy-based routing [323](#)

Port Aggregation Protocol, see PAGP

port authentication [187](#)

and RADIUS [245](#)

IEEE802.1x [190](#), [194](#), [247](#)

MAC authentication [188](#)

port based IGMP [347](#)

port based VLAN type [108](#)

port cloning [455](#), [456](#)

advanced settings [455](#), [456](#)

basic settings [455](#), [456](#)

- port details [97](#)
- port isolation [135](#)
- port mirroring [175, 176, 468](#)
 - direction [176](#)
 - egress [176](#)
 - ingress [176](#)
- port redundancy [178](#)
- port security [197](#)
 - address learning [199](#)
 - limit MAC address learning [199](#)
 - MAC address learning [197](#)
 - overview [197](#)
 - setup [198, 285, 293](#)
- port setup [113](#)
- port status [95](#)
- port VLAN trunking [119](#)
- port-based VLAN [132](#)
 - all connected [135](#)
 - port isolation [135](#)
 - settings wizard [135](#)
- ports
 - "standby" [178](#)
 - diagnostics [424](#)
 - mirroring [175](#)
 - speed/duplex [114](#)
- power
 - voltage [103](#)
- power module
 - current rating [43](#)
 - power wire [43](#)
- power specification [463](#)
- power status [103](#)
- power wires [43](#)
- PPPoE IA [72](#)
 - trusted ports [301](#)
 - untrusted ports [301](#)
- priority level [109](#)
- priority, and OSPF [333](#)
- priority, queue assignment [109](#)
- private VLAN [315](#)
 - configuration [316](#)
 - isolated port [315](#)
 - overview [315](#)
 - promiscuous port [315](#)
- product registration [479](#)
- protocol based VLAN [128](#)

- and IEEE 802.1Q tagging [128](#)
 - example [131](#)
 - hexadecimal notation for protocols [127, 130](#)
 - isolate traffic [128](#)
 - priority [127, 130](#)
- PVID [118, 125](#)
- PVID (Priority Frame) [118](#)

Q

- QoS [468](#)
 - and classifier [201](#)
- queue weight [216](#)
- queuing [215](#)
 - SPQ [216](#)
 - WFQ [216](#)
 - WRR [216](#)
- queuing method [215, 218](#)

R

- RADIUS [244](#)
 - advantages [244](#)
 - and authentication [244](#)
 - Network example [244](#)
 - server [244](#)
 - settings [245](#)
 - setup [245](#)
- Rapid Spanning Tree Protocol, See RSTP. [147](#)
- reboot
 - load configuration [391](#)
- reboot system [391](#)
- redistribute route [340](#)
- reducing routing table size [339](#)
- registration
 - product [479](#)
- related documentation [3](#)
- remote management [420](#)
 - service [421](#)
 - trusted computers [421](#)
- resetting [54, 390](#)
 - to factory default settings [390](#)
- restoring configuration [54, 392](#)
- Reverse Path Forwarding (RPF) [350](#)

- Reverse Path Multicasting (RPM) [349](#)
- RFC 3164 [425](#)
- RIP [340](#)
 - configuration [328](#)
 - direction [327](#)
 - overview [327](#)
 - version [327](#)
 - vs OSPF [331](#)
- RIP (Routing Information Protocol) [327](#)
- Round Robin Scheduling [216](#)
- route cost [340](#)
- router ID [336](#)
- routing domain [110](#), [373](#)
- routing protocols [469](#)
- routing table [453](#)
- RSTP [147](#)
- rubber feet [33](#)

S

- safety warnings [7](#)
- save configuration [54](#), [390](#)
- Secure Shell See SSH
- security [469](#)
- service access control [419](#)
 - service port [420](#)
- sFlow [295](#)
 - collector [297](#)
 - configuration [296](#)
 - datagram [295](#)
 - overview [295](#)
 - poll interval [297](#)
 - sample rate [297](#)
 - UDP port [298](#)
- sFlow agent [295](#)
- sFlow collector [295](#)
- Simple Network Management Protocol, see SNMP
- SNMP [31](#), [398](#)
 - agent [398](#)
 - and MIB [398](#)
 - authentication [410](#), [411](#)
 - communities [408](#)
 - management model [398](#)
 - manager [398](#)
 - MIB [399](#)
 - network components [398](#)
 - object variables [398](#)
 - protocol operations [399](#)
 - security [410](#), [411](#)
 - setup [407](#)
 - traps [409](#)
 - users [410](#)
 - version 3 and security [399](#)
 - versions supported [398](#)
- SNMP traps [400](#)
 - supported [400](#), [401](#), [403](#), [406](#)
- source-based routing [323](#)
- Spanning Tree Protocol, See STP. [147](#)
- SPQ (Strict Priority Queuing) [216](#)
- SSH
 - encryption methods [415](#)
 - how it works [414](#)
 - implementation [415](#)
- SSH (Secure Shell) [413](#)
- SSL (Secure Socket Layer) [415](#)
- standby ports [178](#)
- static bindings [259](#)
- static MAC address [137](#)
- static MAC forwarding [127](#), [129](#), [137](#)
- static multicast address [141](#)
- static multicast forwarding [141](#)
- static route
 - configuration [320](#)
 - overview [319](#)
- static routes [321](#)
- static trunking example [184](#)
- Static VLAN [122](#)
- static VLAN
 - control [124](#)
 - tagging [124](#)
- status [95](#)
 - LED [45](#)
 - link aggregation [179](#)
 - OSPF [334](#)
 - port [95](#)
 - port details [97](#)
 - power [103](#)
 - STP [156](#), [160](#), [166](#)
 - VLAN [121](#)
 - VRRP [372](#)
- STP [147](#), [294](#), [468](#)

- bridge ID [157, 161](#)
- bridge priority [155, 159](#)
- configuration [154, 158, 162](#)
- designated bridge [148](#)
- forwarding delay [155, 159](#)
- Hello BPDU [148](#)
- Hello Time [155, 157, 159, 161](#)
- how it works [148](#)
- Max Age [155, 157, 159, 161](#)
- path cost [148, 156, 160](#)
- port priority [156, 160](#)
- port state [149](#)
- root port [148](#)
- status [156, 160, 166](#)
- terminology [147](#)
- vs loop guard [283](#)
- stub area [331, 338](#)
- stub area, See also OSPF [338](#)
- subnet based VLANs [126](#)
 - and DHCP VLAN [127](#)
 - and priority [126](#)
 - configuration [127](#)
- summary address [339, 341](#)
- switch lockout [54](#)
- switch reset [54](#)
- switch setup [108](#)
- switching [468](#)
- syntax conventions [5](#)
- syslog [263, 425](#)
 - protocol [425](#)
 - server setup [427](#)
 - settings [426](#)
 - setup [426](#)
 - severity levels [425](#)
- system information [102](#)
- system log [423](#)
- system reboot [391](#)

T

- TACACS+ [244](#)
 - setup [247](#)
- TACACS+ (Terminal Access Controller Access-Control System Plus) [243](#)
- tagged VLAN [117](#)
- temperature [464](#)

- temperature indicator [102](#)
- time
 - current [105](#)
 - time zone [105](#)
- Time (RFC-868) [105](#)
- time server [105](#)
- time service protocol [105](#)
 - format [105](#)
- Time To Live (TTL) [351](#)
- trademarks [477](#)
- transceiver
 - installation [39](#)
 - removal [40](#)
- translating RIP into OSPF [340](#)
- traps
 - destination [408](#)
- TRTCM
 - and bandwidth control [358](#)
 - and DiffServ [358](#)
 - color-aware mode [355](#)
 - color-blind mode [355](#)
 - setup [357](#)
- trunk group [177](#)
- trunking [177, 468](#)
 - example [184](#)
- trusted ports
 - ARP inspection [263](#)
 - DHCP snooping [260](#)
 - PPPoE IA [301](#)
- Tunnel Protocol Attribute, and RADIUS [253](#)
- tutorials [63](#)
 - DHCP snooping [63](#)
 - Error Disable [77](#)
 - PPPoE IA [72](#)
- Two Rate Three Color Marker (TRTCM) [354](#)
- Two Rate Three Color Marker, see TRTCM [354](#)
- Type of Service (ToS) [353](#)

U

- UDLD [294](#)
- UniDirectional Link Detection, see UDLD
- untrusted ports
 - ARP inspection [263](#)
 - DHCP snooping [260](#)

PPPoE IA [301](#)
user profiles [244](#)

V

Vendor Specific Attribute See VSA

ventilation holes [34](#)

VID [112](#), [117](#), [121](#), [122](#), [221](#)
 number of possible VIDs [117](#)
 priority frame [117](#)

VID (VLAN Identifier) [117](#)

virtual links [343](#)

virtual links, and OSPF [333](#)

Virtual Router
 status [373](#)

Virtual Router (VR) [371](#)

Virtual Router Redundancy Protocol (VRRP) [371](#)

VLAN [106](#), [117](#), [468](#)
 acceptable frame type [125](#)
 automatic registration [118](#)
 ID [117](#)
 ingress filtering [125](#)
 introduction [106](#)
 number of VLANs [121](#)
 port number [122](#)
 port settings [124](#)
 port-based VLAN [132](#)
 port-based, all connected [135](#)
 port-based, isolation [135](#)
 port-based, wizard [135](#)
 static VLAN [122](#)
 status [121](#), [122](#)
 tagged [117](#)
 trunking [119](#), [125](#)
 type [108](#), [120](#)

VLAN (Virtual Local Area Network) [106](#)

VLAN mapping [287](#)
 activating [288](#)
 configuration [289](#)
 example [287](#)
 priority level [287](#)
 tagged [287](#)
 traffic flow [287](#)
 untagged [287](#)
 VLAN ID [287](#)

VLAN number [112](#)

VLAN stacking [219](#), [221](#)
 configuration [222](#)
 example [219](#)
 frame format [221](#)
 port roles [220](#), [223](#)
 port-based Q-in-Q [223](#)
 priority [221](#)
 selective Q-in-Q [224](#)

VLAN Trunking Protocol, see VTP

VLAN, protocol based, See protocol based VLAN

VLAN, subnet based, See subnet based VLANs
[126](#)

VRID (Virtual Router ID) [372](#)

VRRP [371](#)
 advertisement interval [375](#)
 authentication [374](#)
 backup router [371](#)
 configuration example [377](#)
 Hello message [375](#)
 how it works [371](#)
 interface setup [373](#)
 master router [371](#)
 network example [371](#), [378](#)
 parameters [375](#)
 preempt mode [375](#), [376](#)
 priority [375](#), [376](#)
 status [372](#)
 uplink gateway [376](#)
 uplink status [373](#)
 Virtual Router [371](#)
 Virtual Router ID [376](#)
 VRID [372](#)

VSA [252](#)

VTP [294](#)

W

warranty [479](#)
 note [479](#)

web configurator [31](#), [47](#)
 getting help [56](#)
 layout [48](#)
 login [47](#)
 logout [56](#)
 navigation panel [50](#)

weight, queuing [216](#)

Weighted Round Robin Scheduling (WRR) [216](#)

WFQ (Weighted Fair Queuing) [216](#)

WRR (Weighted Round Robin Scheduling) [216](#)

Z

ZyNOS (ZyXEL Network Operating System) [394](#)